Configuring the Client Adapter

This chapter explains how to change the configuration parameters for a specific profile using ACU.

The following topics are covered in this chapter:

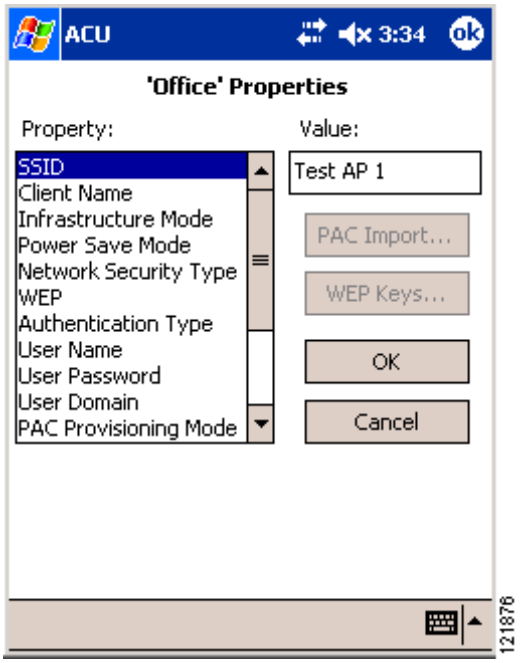
Configuring Your Client Adapter

When you choose to create a new profile or edit an existing profile on the Profiles window, the Properties window appears with the name of your profile in quotation marks. This window enables you to set the configuration parameters for that profile. Follow these steps to access the Properties window and complete the configuration process.

Note If you do not change any of the configuration parameters, the default values are used.

Step 1 When you create or select a profile on the Profiles window and tap the **Edit** button, the Properties window appears (see Figure 5-1).

Figure 5-1 Properties Window



The Property box lists the configuration parameters that can be changed, and the Value box contains the highlighted parameter's current value. The Value box can appear as a drop-down menu with several possible values from which to choose or as a blank field in which characters are to be entered.

Step 2 Table 5-1 lists and describes the client adapter's configuration parameters. Follow the instructions in the table to initially set or change any parameters.

Note The security parameters (Network Security Type, WEP, User Name, User Password, User Domain, PAC Provisioning Mode, and PAC Authority) are listed at the end of the table because they require further action.

Table 5-1 Client Adapter Configuration Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>SSID</td><td>The service set identifier (SSID) identifies the specific wireless network that you want to access.
Range: You can key in up to 32 characters (case sensitive)
Default: A blank field
Note If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the access point management system). 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 cannot access the network.</td></tr>
<tr><td>Client Name</td><td>A logical name for your Windows CE device. It allows 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.
Range: You can enter up to 16 characters
Default: A blank field
Note Each computer on the network should have a unique client name.</td></tr>
<tr><td>Infrastructure Mode</td><td>Specifies the type of network in which your client adapter is installed.
Options: Yes or No
Default: Yes
<table><tr><th>Infrastructure Mode</th><th>Description</th></tr><tr><td>Yes</td><td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td></tr><tr><td>No</td><td>Often referred to as ad hoc or peer-to-peer mode. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point.</td></tr></table></td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Power Save Mode</td><td colspan="2">Sets your client adapter to its optimum power-consumption setting.
Options: CAM, Fast PSP, or Max PSP
Default: Fast PSP (Power Save 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.</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.</td></tr>
<tr><td></td><td>Max PSP (Max Power Savings)</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).</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Authentication Type</td><td>Defines how your client adapter will attempt to authenticate to an access point.

Options: Open or Shared Key

Default: Open

<table>
<tr><th>Authentication</th><th>Description</th></tr>
<tr><td>Open Authentication</td><td>Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. If LEAP, EAP-FAST, or host-based EAP is enabled on your client adapter, Open Authentication is the only available option.</td></tr>
<tr><td>Shared Key Authentication</td><td>Enables your client adapter to communicate only with access points that have the same WEP key. This option is available only if Static WEP Keys is selected.

The access point sends a known unencrypted “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.</td></tr>
</table>
Note Cisco recommends that shared key authentication not be used because it presents a security risk.</td></tr>
<tr><td>Mixed Mode</td><td>Indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations.

• If the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter, you must enable Mixed Mode on the adapter. Otherwise, the client adapter cannot establish a connection with the access point.

• If the access point with which the client adapter is to associate does not have WEP set to Optional, Mixed Mode should be set to Disabled on the adapter.

Options: Enabled or Disabled

Default: Disabled

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.</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>World Mode</td><td>Enables the client adapter to adopt the maximum transmit power level and the frequency range of the access point to which it is associated, provided the access point is also configured for world mode. This parameter is available only in infrastructure mode and is designed for users who travel between countries and want their client adapters to associate to access points in different regulatory domains.

Options: Enabled or Disabled

Default: Disabled

Note When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation’s regulatory agency.</td></tr>
<tr><td>Data Rates</td><td>Specifies the rate at which your client adapter should transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).

Auto is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.

Options: Auto, 1 Mb Only, 2 Mb Only, 5.5 Mb Only, or 11 Mb Only

Default: Auto

<table>
<tr><th>Data Rate</th><th>Description</th></tr>
<tr><td>Auto</td><td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary</td></tr>
<tr><td>1 Mb Only</td><td>Offers the greatest range but the lowest throughput</td></tr>
<tr><td>2 Mb Only</td><td>Offers less range but greater throughput than the 1 Mbps Only option</td></tr>
<tr><td>5.5 Mb Only</td><td>Offers less range but greater throughput than the 2 Mbps Only option</td></tr>
<tr><td>11 Mb Only</td><td>Offers the greatest throughput but the lowest range</td></tr>
</table>
Note Your client adapter’s data rate must be set to Auto or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

Parameter	Description
Transmit Power	Defines the power level at which your client adapter transmits. This value must not be higher than that allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, MKK in Japan, etc.). **Options:** Max, 100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW **Default:** Max (the maximum level programmed into the client adapter and allowed by your country's regulatory agency) **Note** Reducing the transmit power level conserves battery power but decreases radio range. **Note** If the client adapter is running, ACU queries the adapter and displays the settings programmed into the adapter. If the client adapter is not running, ACU displays power level options based on the last known radio type. **Note** When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency. **Note** If you are using an older version of a 350 series client adapter, your power level options may be different than those listed here.
Offline Channel Scan	Causes the client adapter to periodically scan for a better access point with the same SSID if the signal strength falls below 50%. **Options:** Enabled or Disabled **Default:** Enabled

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>WEP</td><td>Specifies the type of wired equivalent privacy (WEP) that your client adapter will use.
Options: No WEP, Static WEP Keys, or Dynamic WEP Keys
Default: No WEP

<table>
<tr><th>WEP</th><th>Description</th></tr>
<tr><td>No WEP</td><td>Disables WEP for your client adapter.</td></tr>
<tr><td>Static WEP Keys</td><td>Enables static WEP for your client adapter after you enter a valid WEP key.
Note Go to Step 3 for instructions on entering a static WEP key and enabling WEP.</td></tr>
<tr><td>Dynamic WEP Keys</td><td>Enables WEP keys to be derived automatically during EAP authentication.
If you set the Network Security Type to LEAP or EAP-FAST, Dynamic WEP Keys is set automatically. If, on a PPC 2002 device, you set the Network Security Type to Host Based EAP, you must set the WEP parameter to Dynamic WEP Keys.
Note Go to Step 3 for instructions on setting dynamic WEP keys.</td></tr>
</table>
</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Network Security Type</td><td>Specifies the type of 802.1X authentication that your client adapter will use.
Options: None, LEAP, EAP-FAST, or Host Based EAP
Default: None
<table>
<tr><th>Network Security Type</th><th>Description</th></tr>
<tr><td>None</td><td>Disables 802.1X authentication for your client adapter.</td></tr>
<tr><td>LEAP</td><td>Specifies that your client adapter use LEAP authentication.
Note Go to Step 3 for instructions on enabling LEAP.</td></tr>
<tr><td>EAP-FAST</td><td>Specifies that your client adapter use EAP-FAST authentication.
Note Go to Step 3 for instructions on enabling EAP-FAST.</td></tr>
<tr><td>LEAP(WPA)</td><td>Specifies that your client adapter use LEAP authentication with Wi-Fi Protected Access (WPA).
Note Go to Step 3 for instructions on enabling LEAP with WPA.</td></tr>
<tr><td>EAP-FAST(WPA)</td><td>Specifies that your client adapter use EAP-FAST authentication with WPA.
Note Go to Step 3 for instructions on enabling EAP-FAST with WPA.</td></tr>
<tr><td>Host Based EAP
(PPC 2002 devices only)</td><td>Specifies that your client adapter use any 802.1X authentication type for which your operating system has support (such as EAP-TLS or PEAP).
Note Go to Step 3 for instructions on enabling host-based EAP.</td></tr>
</table></td></tr>
<tr><td>User Name</td><td>If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the username that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST.
Note Go to Step 3 for instructions on entering the LEAP or EAP-FAST username.</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>User Password</td><td>If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the password that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST.

Note Go to Step 3 for instructions on entering the LEAP or EAP-FAST password.</td></tr>
<tr><td>User Domain</td><td>If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the domain name (if required) that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST.

Note Go to Step 3 for instructions on entering the LEAP or EAP-FAST domain name.</td></tr>
<tr><td>PAC Provisioning Mode</td><td>Enables automatic or manual protected access credentials (PAC) provisioning for this profile. This parameter is available only if the Network Security Type is set to EAP-FAST.

Options: Automatic or Manual

Default: Automatic

<table>
<tr><th>PAC Provisioning Mode</th><th>Description</th></tr>
<tr><td>Automatic</td><td>Enables automatic PAC provisioning. A PAC file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.).</td></tr>
<tr><td>Manual</td><td>Enables manual PAC provisioning. You must select a PAC authority or manually import a PAC file.</td></tr>
</table>
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 key by which authentication transactions are secured.

Note Go to Step 3 for instructions on enabling automatic PAC provisioning or manually importing a PAC file.</td></tr>
</table>

Table 5-1 Client Adapter Configuration Parameters (continued)

Parameter	Description
PAC Authority	Contains the names of all the PAC authorities from which a PAC has previously been provisioned. If this profile is set for manual provisioning, you must select a PAC authority or import a PAC file. This parameter is available only if the Network Security Type is set to EAP-FAST. **Note** Go to Step 3 for instructions on selecting a PAC authority.

Step 3 If you plan to use any of the security features (static WEP, LEAP, EAP-FAST, EAP-TLS, or PEAP), read the "Overview of Security Features" section below and follow the instructions for the security feature you want to activate.

Step 4 Tap **OK** on the Properties window to save any changes you have made. If the profile you just edited is the active profile and your client adapter is inserted, the changes are applied immediately.

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 EAP authentication process. The information in the "Static WEP Keys" and "Dynamic WEP Keys with EAP" sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

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

Note Refer to the "Additional WEP Key Security Features" section on page 5-16 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

Each device (or profile) 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; however, you do not need to re-enter them each time the client adapter is inserted or the Windows CE device is reset. 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.

The ACU Properties window 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 as well as to enable or disable static WEP. Refer to the "Using Static WEP" section on page 5-20 for instructions.

Dynamic WEP Keys with EAP

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.

Up to three 802.1X authentication types can be selected in ACU for use with Windows CE devices:

- **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 later, Cisco Access Registrar version 1.7 and later, and Funk Software's Steel-Belted RADIUS version 3.0 and later.

  LEAP is enabled in ACU, and either a saved LEAP username and password are entered in ACU or a temporary LEAP username and password are entered in WLM. The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The temporary LEAP username and password are stored in the client adapter's volatile memory and need to be re-entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) is available on PPC 2002, PPC 2003, and Windows CE .NET 4.2 devices. EAP-FAST 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.

  EAP-FAST is enabled in ACU, and either a saved EAP-FAST username and password are entered in ACU or a temporary EAP-FAST username and password are entered in WLM. In addition, automatic or manual PAC provisioning is enabled in ACU. The client adapter uses the username, password, and PAC to perform mutual authentication with the RADIUS server through the access point. The temporary EAP-FAST username and password are stored in the client adapter's volatile memory and need to be re-entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset.

  PACs are created by Cisco Secure ACS and are identified by an ID. The user obtains a copy of the PAC from the server, and the ID links the PAC to the profile created in ACU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device. The following rules govern PAC storage:

  – PACs are stored in a single PAC database and are available to all users of the device.

  – PAC files can be added or replaced using the import feature, but they cannot be removed or exported.

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.

- **Host Based EAP** (PPC 2002 devices only)—Selecting this option enables you to use any 802.1X authentication type for which your Windows CE device has support, such as EAP-TLS or PEAP. You can select this option only on PPC 2002 devices with the 802.1X backport installed.

Note PPC 2003 and other Windows CE .NET 4.2 devices can be configured for EAP-TLS or PEAP authentication if you configure your client adapter through Windows CE .NET instead of ACU. See Appendix E for instructions.

  - **EAP-TLS**—EAP-TLS is enabled or disabled through the Authentication Manager and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-TLS requires the use of certificates 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.

  - **Cisco PEAP**—Cisco PEAP authentication (also known as *PEAP-GTC*) 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. Cisco PEAP is enabled or disabled through the Authentication Manager and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. Cisco PEAP requires you to enter your username and password in order to start the authentication process and gain access to the network. RADIUS servers that support Cisco PEAP authentication include Cisco Secure ACS version 3.1 or later.

Note To use Cisco PEAP authentication, you must have checked the **Install Cisco PEAP Support** check box during installation.

When you enable Network-EAP or Require EAP on your access point and configure your client adapter for LEAP, EAP-FAST, EAP-TLS, or PEAP, 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 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), password and PAC (EAP-FAST), or certificate (EAP-TLS) being the shared secret for authentication. The password or PAC 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 one of these sections for instructions on enabling EAP authentication:

- Enabling LEAP, page 5-22
- Enabling EAP-FAST, page 5-24
- Enabling Host-Based EAP, page 5-28

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 certification that greatly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and compatible with the 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.

Using WPA key management, 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.

When you configure your client adapter through ACU, only 350 series cards that are installed in Windows CE .NET 4.2 devices and running LEAP or EAP-FAST authentication can be used with WPA. Support for WPA is available in client adapter driver and utility version 2.60 or later.

Refer to one of these sections for instructions on enabling LEAP or EAP-FAST authentication with WPA:

- Enabling LEAP, page 5-22
- Enabling EAP-FAST, page 5-24

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 seamless roaming to prevent delays and gaps in conversation. Support for fast roaming is available for LEAP- or EAP-FAST-enabled clients in firmware version 5.40.10.

During normal operation, LEAP- or EAP-FAST-enabled clients mutually authenticate with a new access point by performing a complete LEAP or EAP-FAST authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for fast roaming, LEAP- or EAP-FAST-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 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.

This feature does not need to be enabled on the client adapter; it is supported automatically in client adapter firmware version 5.40.10. However, it must be enabled on the access point.

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 or EAP-FAST Authentication

The following client adapter and access point firmware versions support a feature that is designed to detect access points that fail LEAP or EAP-FAST authentication:

- Client adapter firmware version 5.40.10
- 12.00T or later (340, 350, and 1200 series access points)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)

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

The process takes place as follows:

1. A client with a LEAP or EAP-FAST profile attempts to associate to access point A.
2. Access point A does not handle LEAP or EAP-FAST authentication successfully, perhaps because the access point does not understand LEAP or EAP-FAST or cannot communicate to a trusted LEAP or EAP-FAST 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 in the firmware of both devices. However, both the client and access point must use these firmware 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 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 driver and firmware. However, they must be enabled on the access point.

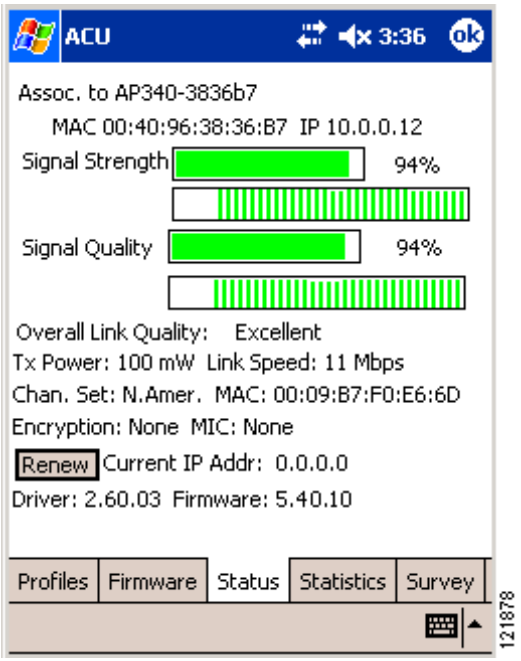
Note Access point firmware version 11.10T or later is required to enable these security features. Refer to the software configuration guide for your access point for instructions on enabling these features.

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

The Status window indicates if MIC is supported by the client adapter's driver and is enabled on the access point. See Figure 5-2.

Figure 5-2 Status Window



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, EAP-FAST, EAP-TLS, or PEAP authentication can associate to the access point. Client devices using static WEP (with open or shared key 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 5-2 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 documentation for your access point for instructions on enabling any of these features on the access point.

Table 5-2 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID
LEAP authentication with WPA (on Windows CE .NET 4.2 devices only)	Enable LEAP(WPA)	Select a cipher suite that includes TKIP, set up and enable WEP, 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-FAST authentication	Enable EAP-FAST and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable Network-EAP for the SSID

Table 5-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-FAST authentication with WPA (on Windows CE .NET 4.2 devices only)	Enable EAP-FAST(WPA) and enable automatic provisioning or import a PAC file	Select a cipher suite that includes TKIP, set up and enable WEP, 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		
If using ACU to configure card (on PPC 2002 devices)	Enable Host Based EAP and Dynamic WEP Keys in ACU and select TLS as the EAP Type in the Authentication Manager	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
If using Windows CE .NET to configure card (on PPC 2003 and Windows CE .NET 4.2 devices)	Select Enable 802.1X Authentication on This Network and TLS as the EAP Type	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
PEAP authentication		
If using ACU to configure card (on PPC 2002 devices)	Enable Host Based EAP and Dynamic WEP Keys in ACU and select Cisco PEAP (or PEAP if the Microsoft PEAP supplicant is installed) as the EAP Type in the Authentication Manager	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
If using Windows CE .NET to configure card (on PPC 2003 and Windows CE .NET 4.2 devices)	Select Enable 802.1X Authentication on This Network and Cisco PEAP (or PEAP, which denotes the Microsoft PEAP supplicant) as the EAP Type	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
Fast roaming (CCKM)	Enable LEAP or EAP-FAST and use firmware version 5.40.10	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. **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.

Table 5-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
Fast roaming (CCKM) with TKIP	Enable LEAP(WPA) or EAP-FAST(WPA) and use firmware version 5.40.10	Use firmware version 12.2(11)JA or later, select a cipher suite that includes TKIP, and enable Network-EAP and CCKM for the SSID. **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 or EAP-FAST authentication	No settings required; automatically enabled in firmware version 5.40.10	No settings required; automatically enabled in the following firmware versions: 12.00T or later (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA or later (1100 series access points)
MIC	Automatically enabled in driver	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	Automatically enabled in firmware	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-FAST, EAP-TLS, or PEAP	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.

Enabling Static WEP and Entering a New Static WEP Key

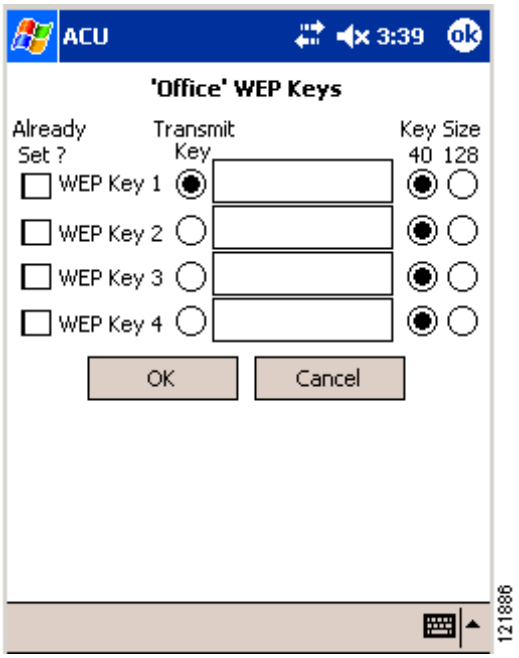
Follow these steps to enter a new static WEP key for this profile.

Step 1 From the Properties window, select **Network Security Type** under Property and **None** from the list of options in the Value box.

Step 2 Select **WEP** under Property and **Static WEP Keys** from the list of options in the Value box.

Step 3 Tap the **WEP Keys** button. The WEP Keys window appears (see Figure 5-3).

Figure 5-3 WEP Keys Window



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

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 grayed out, and you are unable to select it.

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 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 6 Tap 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 Tap **OK** to write your WEP key(s) to the client adapter's volatile memory and the registry of the Windows CE device or tap **Cancel** to exit the WEP Keys window without updating the keys.

Step 8 Tap **OK** to save your changes.

Overwriting an Existing Static WEP Key

Follow these steps to overwrite an existing static WEP key.

Step 1 From the Properties window, tap the **WEP Keys** button. The WEP Keys window appears (see Figure 5-3). A check mark 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 window. 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 Tap within the blank field of that key.

Step 4 Enter a new key, following the guidelines outlined in Step 5 of the "Enabling Static WEP and Entering a New Static WEP Key" section on page 5-20.

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 Tap **OK** to write your new static WEP key to the client adapter's volatile memory and the registry of the Windows CE device or tap **Cancel** to exit the WEP Keys window without overwriting any keys.

Step 7 Tap **OK** to save your changes.

Disabling Static WEP

Follow these steps if you ever need to disable static WEP.

Note Selecting LEAP for the Network Security Type disables static WEP automatically.

Step 1 Double-tap the **ACU** icon or select **Start** > **Programs** > **Cisco** > **ACU**. The Profiles window appears.

Step 2 Select the profile that you want to change from the Manage Profiles box and tap the **Edit** button.

Step 3 Select **WEP** under Property and **No WEP** from the list of options in the Value box.

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

Enabling LEAP

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

- Client adapters must support WEP.
- To use WPA, 350 series client adapters must be installed in Windows CE .NET 4.2 devices and use client adapter driver and utility version 2.60 or later.
- 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), or Cisco IOS Release 12.2(4)JA (1100 series access points).

  Note To use WPA or fast roaming (CCKM), access points must use Cisco IOS Release 12.2(11)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication and Fast Roaming features, access points must use the firmware versions listed on page 5-14.

- All necessary infrastructure devices such as access points and servers must be properly configured for LEAP authentication.

Note Cisco recommends the use of strong passwords for LEAP authentication in order to minimize the risk of successful attacks by rogue access points. Refer to the "Creating Strong Passwords" section on page 9-4 for tips on creating strong passwords.

Follow these steps to enable LEAP authentication for this profile.

Step 1 From the Properties window, select **Network Security Type** under Property and **LEAP** or **LEAP(WPA)** from the list of options in the Value box. When LEAP or LEAP(WPA) is enabled, the following parameters on the Properties window are changed automatically:

- WEP is set to Dynamic WEP Keys.
- Authentication Type is set to Open.

Note If you select LEAP(WPA), TKIP is used for data encryption, and the Encryption field on the ACU Status window shows WPA TKIP.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 5-14 for additional information.

Step 2 Perform one of the following:

- If you want to use a temporary username and password (which must be entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset in order to authenticate and gain access to the network), go to Step 3.
- If you want to use a saved username and password (which do not need to be entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset because authentication occurs automatically as needed using your saved credentials), enter your LEAP username, password, and optional domain name in the User Name, User Password, and User Domain edit boxes.

Note Usernames are limited to 64 ASCII characters, and passwords are limited to 32 ASCII characters. However, if a domain name is entered in the User Domain field, the sum of the username and domain name is limited to 63 ASCII characters.

Step 3 Tap **OK** to enable LEAP.

Step 4 Refer to the "Using LEAP or EAP-FAST" section on page 6-2 for instructions on authenticating using LEAP.

Enabling EAP-FAST

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

- 350 series client adapters must be installed on a PPC 2002, PPC 2003, or Windows CE .NET 4.2 device.
- Client adapters must support WEP and use firmware version 5.40.10.
- To use WPA, client adapters must be installed in Windows CE .NET 4.2 devices and use client adapter driver and utility version 2.60 or later.
- 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), or Cisco IOS Release 12.2(4)JA (1100 series access points).

Note To use WPA or fast roaming (CCKM), access points must use Cisco IOS Release 12.2(11)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication and Fast Roaming features, access points must use the firmware versions listed on page 5-14.

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

Obtaining a PAC File (Manual PAC Provisioning Only)

If you are planning to enable manual PAC provisioning for this EAP-FAST profile, you must obtain a PAC file before you can import it for use on your Windows CE device. Follow these steps if you have not yet obtained a PAC file.

Step 1 Obtain the PAC file (*.pac) from your system administrator.

Step 2 Establish an ActiveSync connection between your laptop or PC and your Windows CE device.

Step 3 Use **Windows Explorer** to copy the PAC file and paste it into a folder under **My Computer** > **Mobile Device**.

Note For PPC devices, the destination must be either the Business or Personal folder.

Step 4 Follow the steps in the "Enabling EAP-FAST" section below to import the PAC file for your Windows CE device.

Enabling EAP-FAST

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

Step 1 From the Properties window, select **Network Security Type** under Property and **EAP-FAST** or **EAP-FAST(WPA)** from the list of options in the Value box. When EAP-FAST or EAP-FAST(WPA) is enabled, the following parameters on the Properties window are changed automatically:

- WEP is set to Dynamic WEP Keys.
- Authentication Type is set to Open.

Note If you select EAP-FAST(WPA), TKIP is used for data encryption, and the Encryption field on the ACU Status window shows WPA TKIP.

Note Refer to the "Wi-Fi Protected Access (WPA)" section on page 5-14 for additional information.

Step 2 Perform one of the following:

- If you want to use a temporary username and password (which must be entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset in order to authenticate and gain access to the network), go to Step 3.
- If you want to use a saved username and password (which do not need to be entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset because authentication occurs automatically as needed using your saved credentials), enter your EAP-FAST username, password, and optional domain name in the User Name, User Password, and User Domain edit boxes.

Note Usernames are limited to 64 ASCII characters, and passwords are limited to 32 ASCII characters. However, if a domain name is entered in the User Domain field, the sum of the username and domain name is limited to 63 ASCII characters.

Step 3 Perform one of the following:

- If you want to enable automatic PAC provisioning, select **PAC Provisioning Mode** under Property and **Automatic** from the list of options in the Value box. A protected authentication credentials (PAC) file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.). This is the default setting. If you select this option, go to Step 5.
- If you want to enable manual PAC provisioning, select **PAC Provisioning Mode** under Property and **Manual** from the list of options in the Value box. You must select a PAC authority or manually import a PAC file. If you select this option, go to Step 4.

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.

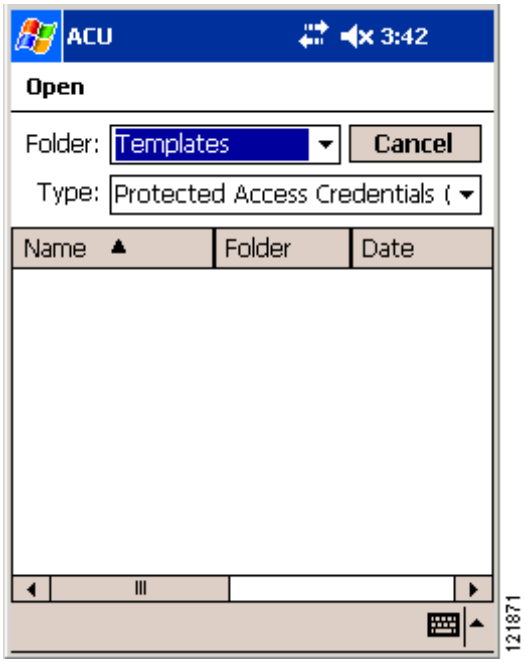
Note Provisioning occurs only upon initial negotiation of the PAC or upon PAC expiration. After the PAC is provisioned, it serves as the key by which authentication transactions are secured.

Step 4 Perform one of the following to enable manual PAC provisioning:

- Select **PAC Authority** under Property and select the PAC authority associated with the profile's SSID from the list of options in the Value box. The list contains the names of all the PAC authorities from which PACs have previously been provisioned.
- If the PAC authority list is empty or does not contain the name of a desired PAC authority, follow these steps to import a PAC file:

  a. Tap the **PAC Import** button. The Open window appears (see Figure 5-4).

Figure 5-4 Open Window



b. Select the folder where the PAC file is located from the Folder drop-down menu. Then tap the file (*.pac) in the Name field in the center of the window.

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

c. If the PAC Password window appears (see Figure 5-5), enter the PAC file password and tap **OK**.

Figure 5-5 PAC 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.

d. 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 replace the existing PAC. If you tap **Yes**, the existing PAC is replaced by the new one from the imported file.

e. The PAC file is imported, and the PAC authority that issued the PAC file is added to the PAC authority list as the active PAC authority.

Step 5 Tap **OK** to enable EAP-FAST. If you imported a PAC file, it is now added to your PAC database.

Step 6 Refer to the "Using LEAP or EAP-FAST" section on page 6-2 for instructions on authenticating using EAP-FAST.

Enabling Host-Based EAP

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

- The Windows CE device must be a PPC 2002 device.

Note PPC 2003 and other Windows CE .NET 4.2 devices can be configured for EAP-TLS or PEAP authentication if you configure your client adapter through Windows CE .NET instead of ACU. See Appendix E for instructions.

- Client adapters must support WEP.
- Access points to which your client adapter will attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 12.2(4)JA (1100 series access points), or 11.54T (1200 series access points).
- All necessary infrastructure devices such as access points, servers, gateways, and user databases must be properly configured for the authentication type you plan to enable on the client.

Obtaining and Importing CA and User Certificates

EAP-TLS and PEAP authentication require the use of certificates. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. After you import the necessary certificates, you should not have to repeat this procedure until the certificates expire (at a time that is predetermined by the certificate server).

Note Chapter 8 provides instructions for viewing and removing certificates, if necessary.

Obtaining CA and User Certificates

If you have not yet obtained a CA certificate (for EAP-TLS or PEAP) and a user certificate (for EAP-TLS), follow these steps.

Step 1 Obtain the certificate file(s) (*.cer or *.crt) from your system administrator.

Step 2 Establish an ActiveSync connection between your laptop or PC and your Windows CE device.

Step 3 Open **Windows Explorer** on your laptop or PC.

Step 4 Copy the certificate file(s) and paste them into a folder under **My Computer** > **Mobile Device**.

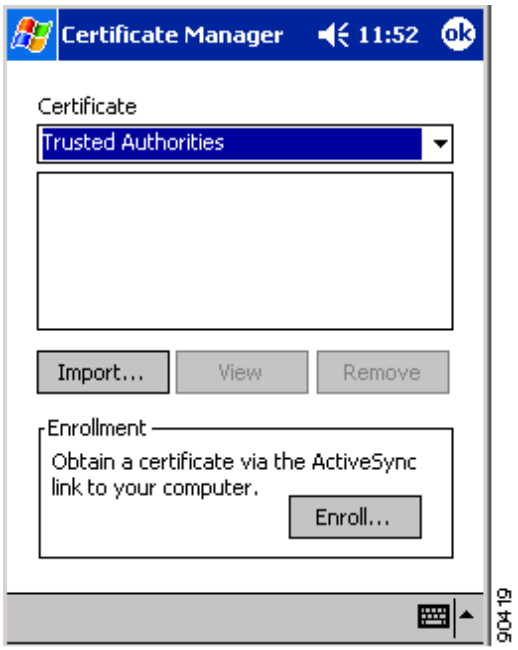
Step 5 Follow the steps in the "Importing a CA Certificate" section on page 5-29 and the "Importing a User Certificate" section on page 5-30 to import the certificate file(s) for your Windows CE device.

Importing a CA Certificate

If you are planning to use EAP-TLS or PEAP authentication on a PPC 2002 device, follow these steps to import the CA certificate.

Step 1 Select **Start** > **Programs** > **Cisco** > **CertMgr**. The Certificate Manager window appears (see Figure 5-6).

Figure 5-6 Certificate Manager Window

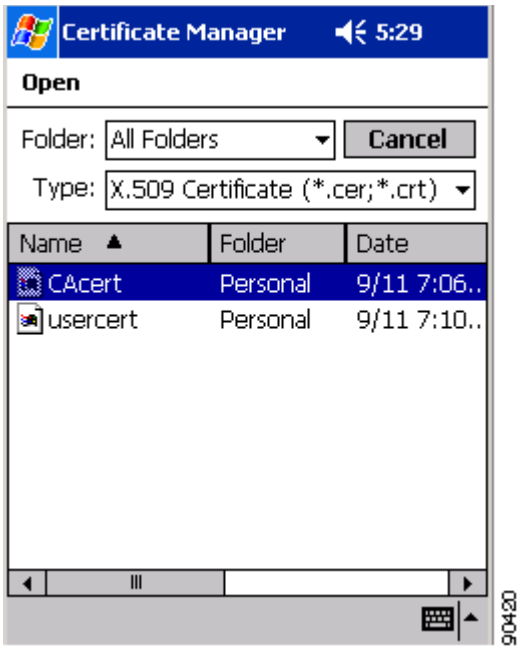


Step 2 Make sure **Trusted Authorities** appears in the Certificate drop-down menu.

Step 3 Tap the **Import** button.

Step 4 The Certificate Manager Open window appears (see Figure 5-7).

Figure 5-7 Certificate Manager Open Window



Step 5 Tap the CA certificate file.

Step 6 The Certificate Manager window reappears with the name of the CA certificate server listed in the middle of the window.

Step 7 Tap **OK** to close the Certificate Manager.

Importing a User Certificate

If you are planning to use EAP-TLS authentication on a PPC 2002 device, follow these steps to import the user certificate.

Note As an alternative to the procedure below, you can use the Certificate Manager to import a user certificate. To do so, follow the steps in the "Importing a CA Certificate" section above, but make sure My Certificates (not Trusted Authorities) appears in the Certificate drop-down menu in Step 2 and tap the user certificate file (not the CA certificate file) in Step 5.

Step 1 Make sure that your Windows CE device has an ActiveSync link to a laptop or PC that is on the same network as the certificate server you want to use.

Step 2 Select **Start** > **Programs** > **Cisco** > **Enroll**. The Certificate Enrollment window appears (see Figure 5-8).

Figure 5-8 Certificate Enrollment Window

Step 3 Enter your username, password, and server name for your certificate server, which can be obtained from your system administrator, in the appropriate fields.

Step 4 Tap the **Enroll** button. The box at the bottom of the window indicates the status of the certificate enrollment by changing from *Ready* to *Processing*.

If the operation is successful, the following message appears: "A certificate has been added to your device."

Step 5 Tap **OK** to close the Certificate Enrollment window.

Enabling Host-Based EAP

Follow these steps to enable host-based EAP authentication (EAP-TLS or PEAP) for this profile on a PPC 2002 device.

Note Because EAP-TLS and PEAP authentication are not enabled in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. You can create a profile in ACU that uses host-based EAP, but you must enable the specific authentication type in the Authentication Manager. In addition, only one authentication type can be set at a time; therefore, if you have more than one profile in ACU that uses host-based EAP and you want to use another authentication type, you must change the authentication type in the Authentication Manager after switching profiles in ACU.

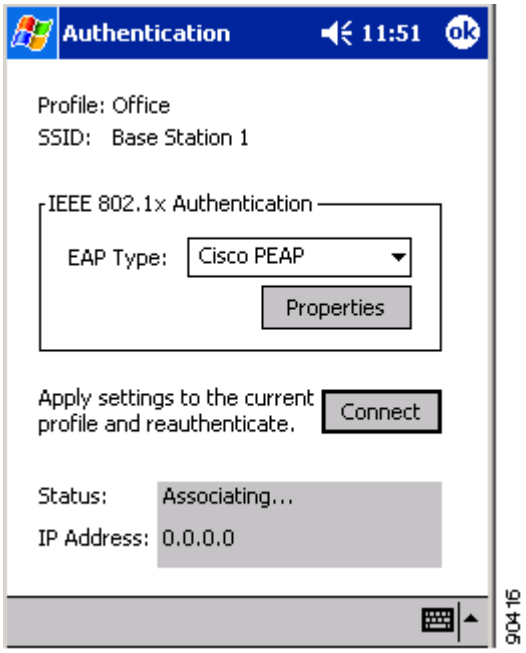
Step 1 From the Properties window, select **Network Security Type** under Property and **Host Based EAP** from the list of options in the Value box.

Step 2 Select **WEP** under Property and **Dynamic WEP Keys** from the list of options in the Value box.

Step 3 Tap **OK** to save your changes.

Step 4 Select **Start** > **Programs** > **Cisco** > **AuthMgr**. The Authentication window appears (see Figure 5-9).

Figure 5-9 Authentication Window



Step 5 Perform one of the following, depending on the authentication type you want to use:

- If you are planning to use EAP-TLS, go to the "Enabling EAP-TLS" section below.
- If you are planning to use PEAP, go to the "Enabling PEAP" section on page 5-33.

Enabling EAP-TLS

Follow these steps to enable EAP-TLS for this profile.

Step 1 For EAP Type, select **TLS**.

Step 2 If your Windows CE device has more than one user certificate, tap the **Properties** button. On the Select Certificate window, select the user certificate that you want to use and tap **OK**.

Step 3 The configuration is complete. Tap the **Connect** button on the Authentication window to start the EAP authentication process.

Note Any time you make a change to the active profile in ACU or the Authentication Manager, you must tap the **Connect** button on the Authentication window to start the authentication process.

Step 4 Refer to the "Using EAP-TLS" section on page 6-5 for instructions on authenticating using EAP-TLS.

Enabling PEAP

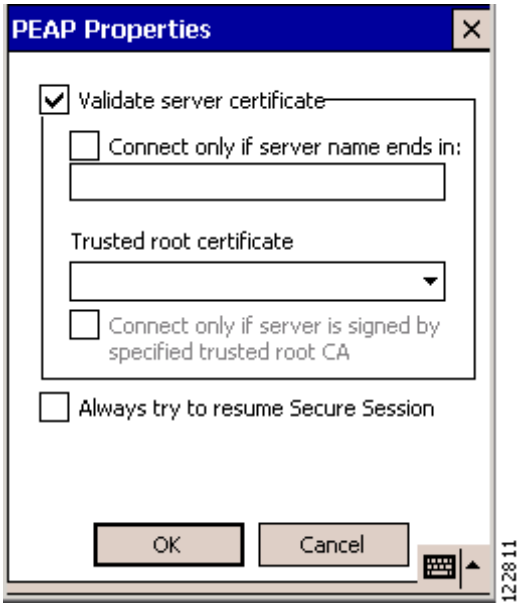
Follow these steps to enable PEAP for this profile.

Step 1 For EAP Type, select **Cisco PEAP** or **PEAP**. If you select Cisco PEAP, go to Step 2. If you select PEAP, go to Step 9.

Note **PEAP** appears as an EAP Type option on a PPC 2002 device if the Microsoft PEAP supplicant (rather than the Cisco PEAP supplicant) is installed.

Step 2 Tap the **Properties** button. The PEAP Properties window appears (see Figure 5-10).

Figure 5-10 PEAP Properties Window



Step 3 Make sure that the **Validate server certificate** check box is checked if server certificate validation is required (recommended).

Step 4 If you want to specify the name of the server to connect to, check the **Connect only if server name ends in** check box and enter the appropriate server name suffix in the field below.

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

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

Step 5 Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate field. If necessary, tap the arrow on the drop-down menu and select the appropriate name.

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

Step 6 Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.

Step 7 Perform one of the following:

- Check the **Always try to resume Secure Session** check box if you want the PEAP protocol to always attempt to resume the previous session before prompting you to re-enter your credentials.
- Uncheck the **Always try to resume Secure Session** check box if you want to be prompted to re-enter your username and password whenever your client adapter's radio becomes disassociated (for example, when the card is ejected, the radio is turned off, you wander out of range of an access point, you switch profiles, and so on).

Note Checking this check box gives you the convenience of not having to re-enter your username and password when your client adapter experiences momentary losses of association. The PEAP Session Timeout setting on the Cisco Secure ACS System Configuration - Global Authentication Setup window controls how long the resume feature is active (that is, the amount of time during which the PEAP session can be resumed without re-entering user credentials). If you leave your device unattended during this timeout period, be aware that someone can resume your PEAP session and access the network.

Step 8 Tap **OK** to save your settings. The configuration is complete.

Step 9 Tap the **Connect** button on the Authentication window to start the EAP authentication process.

Note Any time you make a change to the active profile in ACU or the Authentication Manager, you must tap the **Connect** button on the Authentication window to start the authentication process.

Step 10 Refer to the "Using PEAP" section on page 6-6 for instructions on authenticating using PEAP.

Disabling LEAP, EAP-FAST, or Host-Based EAP

Follow these steps to disable LEAP, EAP-FAST, or host-based EAP (EAP-TLS or PEAP) for a particular profile on a PPC 2002 device.

Step 1 Double-tap the **ACU** icon or select **Start** > **Programs** > **Cisco** > **ACU**. The Profiles window appears.

Step 2 Select the profile that you want to change from the Manage Profiles box and tap the **Edit** button.

Step 3 Select **Network Security Type** under Property and **None** from the list of options in the Value box.

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