APPENDIX E

Configuring the Client Adapter through the Windows XP Operating System

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

The following topics are covered in this appendix:

Overview

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

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

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

Overview of Security Features

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

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

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

Static WEP Keys

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

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

EAP (with Dynamic WEP Keys)

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

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

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

  RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.

- **Protected EAP** (or **PEAP**)—One of the following PEAP authentication types are available, depending on the software that is installed on your computer:

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

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

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

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

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

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

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

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

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

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

Note Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ab.html

WPA

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

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

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

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

Configuring the Client Adapter

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

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

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

Step 1 Make sure the client adapter's driver has been installed and the client adapter is inserted in the Windows XP device.

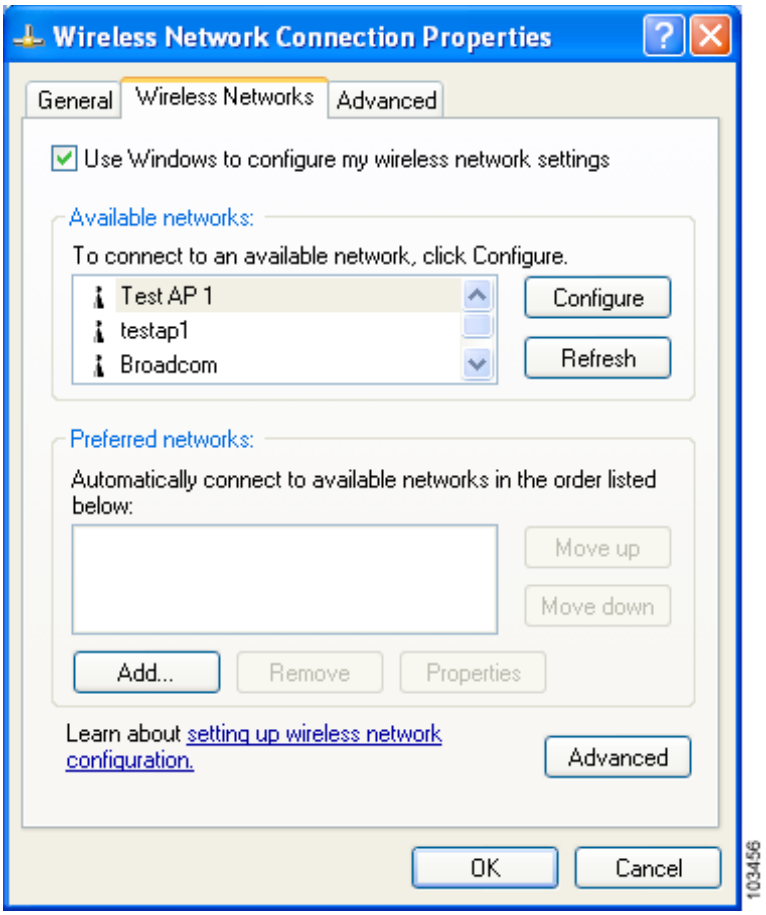
Step 2 Double-click **My Computer**, **Control Panel**, and **Network Connections**.

Step 3 Right-click **Wireless Network Connection**.

Step 4 Click **Properties**. The Wireless Network Connection Properties window appears.

Step 5 Click the **Wireless Networks** tab. The following window appears (see Figure E-1).

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



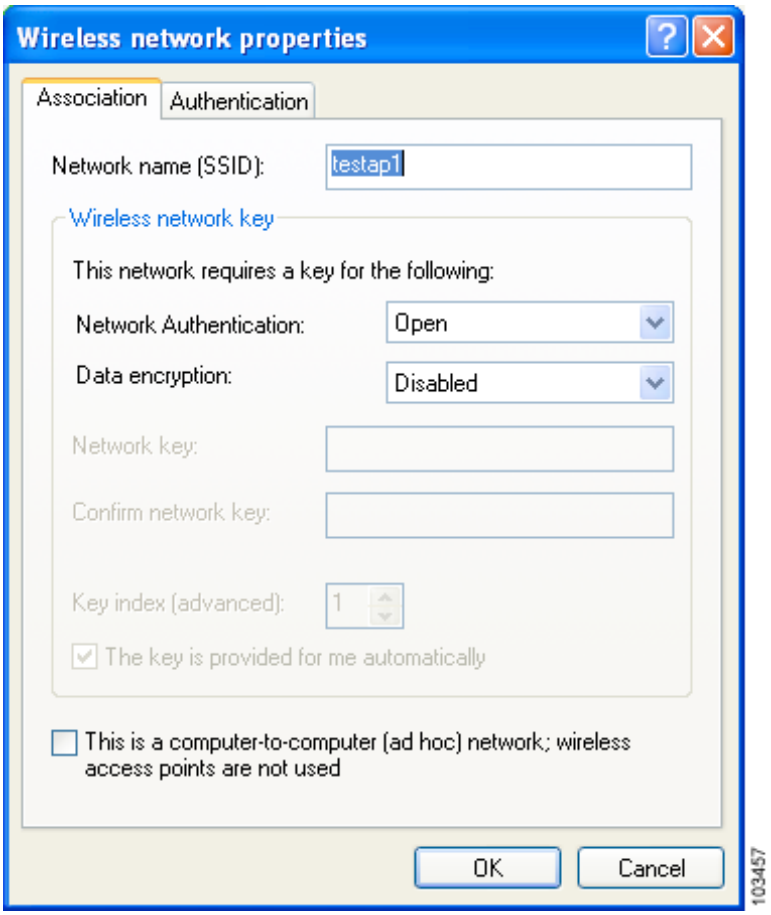
Step 6 Make sure that the **Use Windows to configure my wireless network settings** check box is checked.

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

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

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

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



Step 8 Perform one of the following:

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

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

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

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

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

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

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

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

Note Refer to the "WPA" section on page E-4 for more information on WPA and WPA-PSK.

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

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

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

Note If you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP, go to Step 13.

a. Make sure the **The key is provided for me automatically** check box is unchecked.

b. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

    Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

    Example: 5A5831353335545955493335 34 (hexadecimal) or ZX1535TYUI354 (ASCII)

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

- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.

c. In the Key index (advanced) field, choose the number of the WEP key you are creating (**1**, **2**, **3**, or **4**).

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

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

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

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

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

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

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

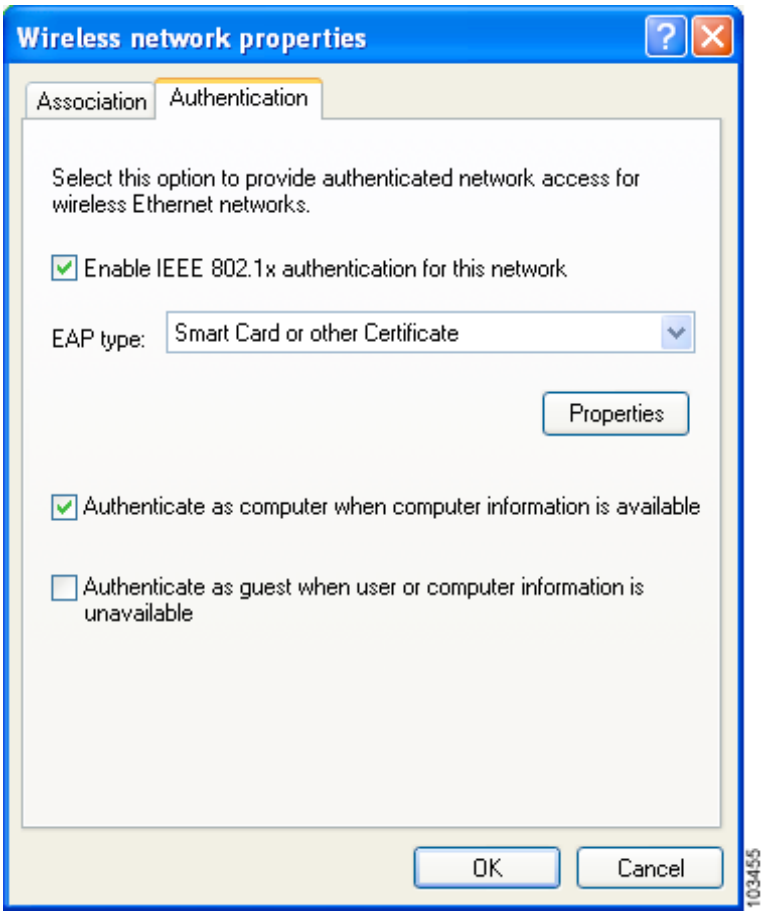
- If you are planning to use EAP-TLS authentication, follow the instructions in the "Enabling EAP-TLS Authentication" section on page E-10.
- If you are planning to use PEAP authentication, follow the instructions in the "Enabling PEAP Authentication" section on page E-13.

Enabling EAP-TLS Authentication

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

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

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

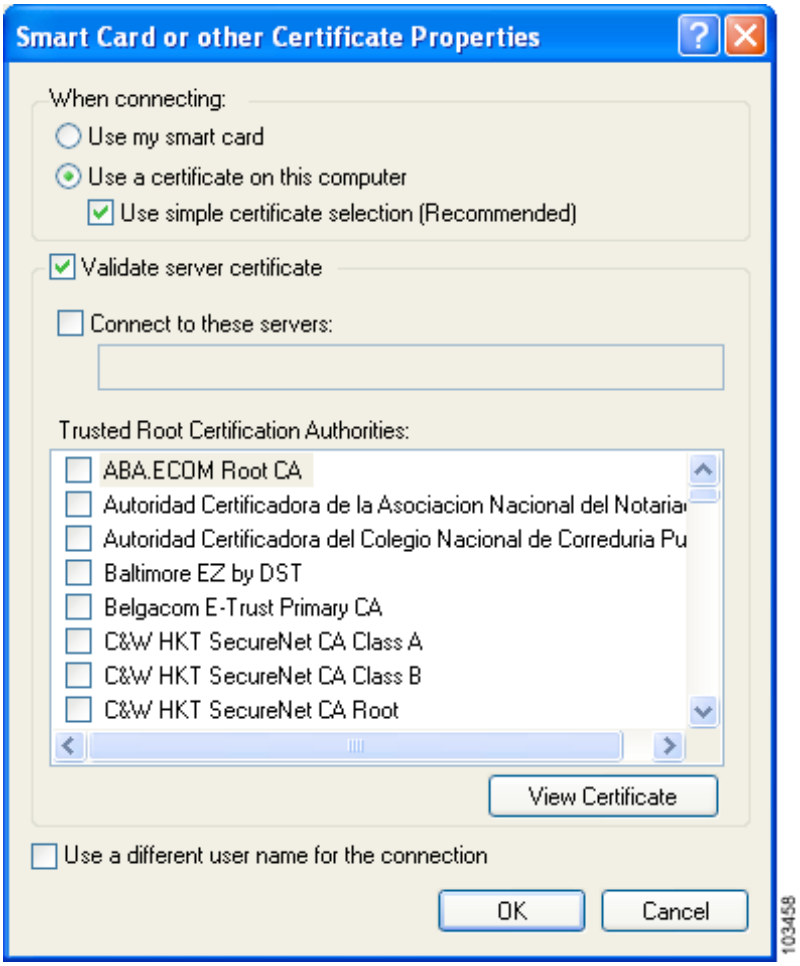


Step 2 Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.

Step 3 For EAP type, choose **Smart Card or other Certificate**.

Step 4 Click **Properties**. The Smart Card or other Certificate Properties window appears (see Figure E-4).

Figure E-4 Smart Card or other Certificate Properties Window



Step 5 Choose the **Use a certificate on this computer** option.

Step 6 Check the **Use simple certificate selection (Recommended)** check box.

Step 7 Check the **Validate server certificate** check box if server certificate validation is required.

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

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

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

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

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

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

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

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

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

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

The client adapter should now EAP authenticate.

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

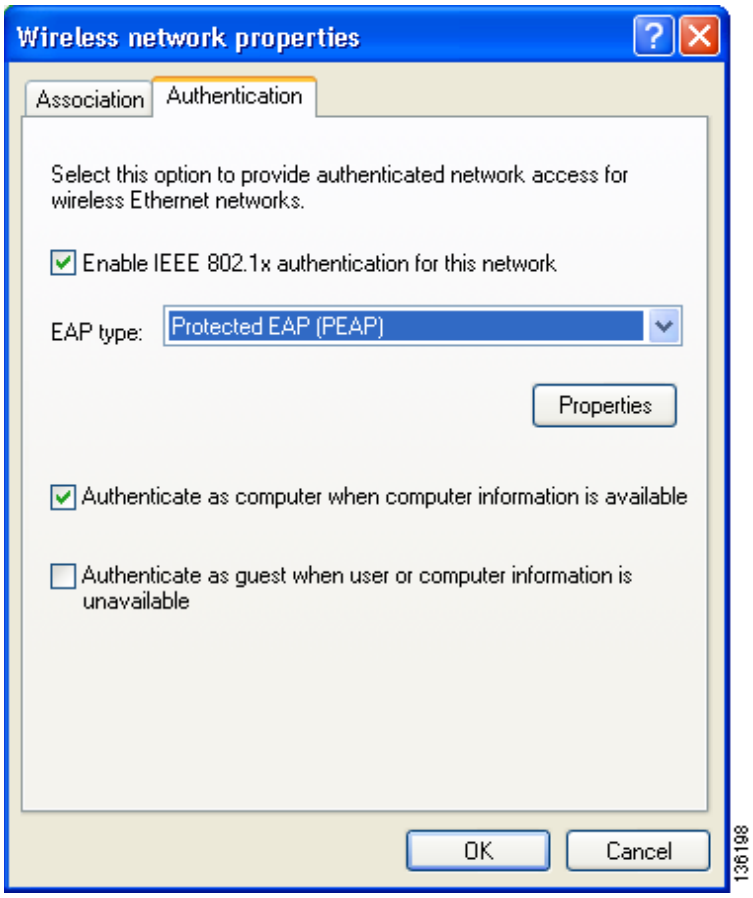
Step 14 To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication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

Enabling PEAP Authentication

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

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

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



Step 2 Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.

Step 3 For EAP type, choose one of the following, depending on the software that is installed on your computer:

- **Protected EAP (PEAP)**—This option appears for PEAP (EAP-MSCHAP V2).
- **PEAP**—This option appears for PEAP (EAP-GTC).

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

Step 4 Perform one of the following:

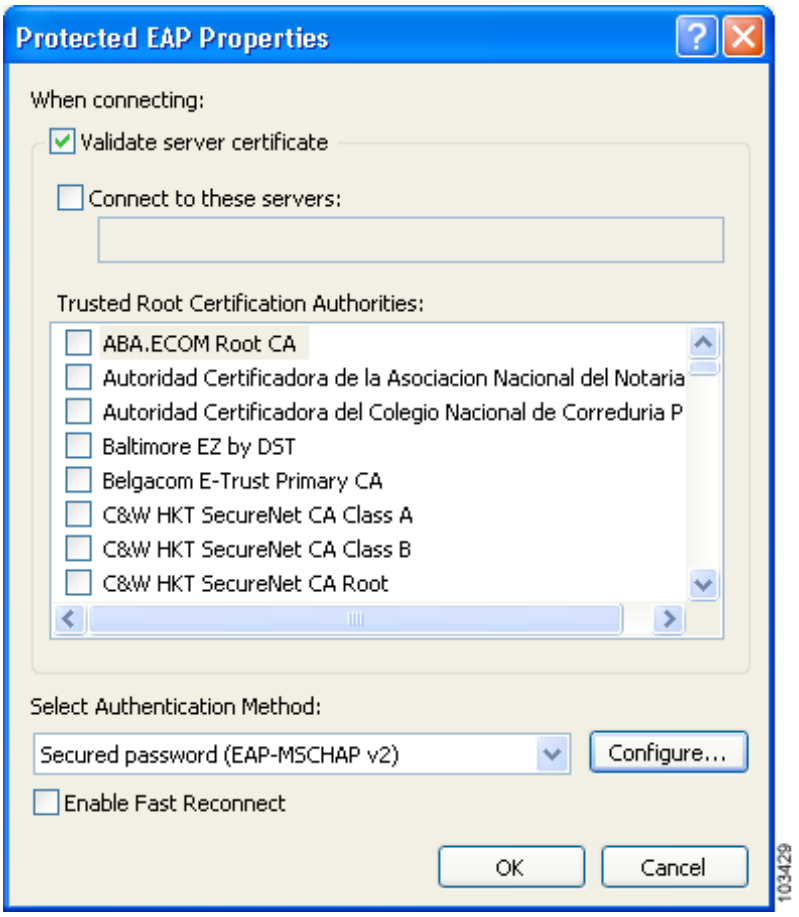
- If you chose Protected EAP (PEAP), follow the instructions in the "Enabling PEAP (EAP-MSCHAP V2)" section below.
- If you chose PEAP, follow the instructions in the "Enabling PEAP (EAP-GTC)" section on page E-16.

Enabling PEAP (EAP-MSCHAP V2)

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

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

Figure E-6 Protected EAP Properties Window



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

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

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

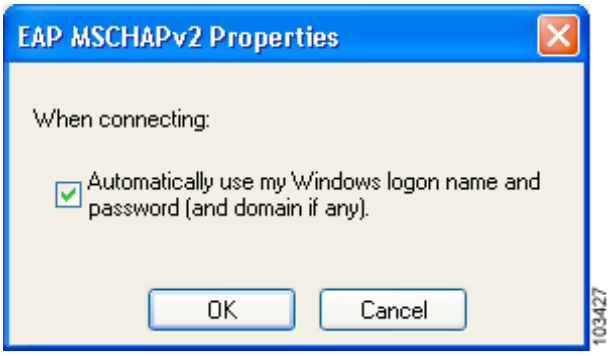
Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

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

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

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

Figure E-7 EAP MSCHAPv2 Properties Window



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

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

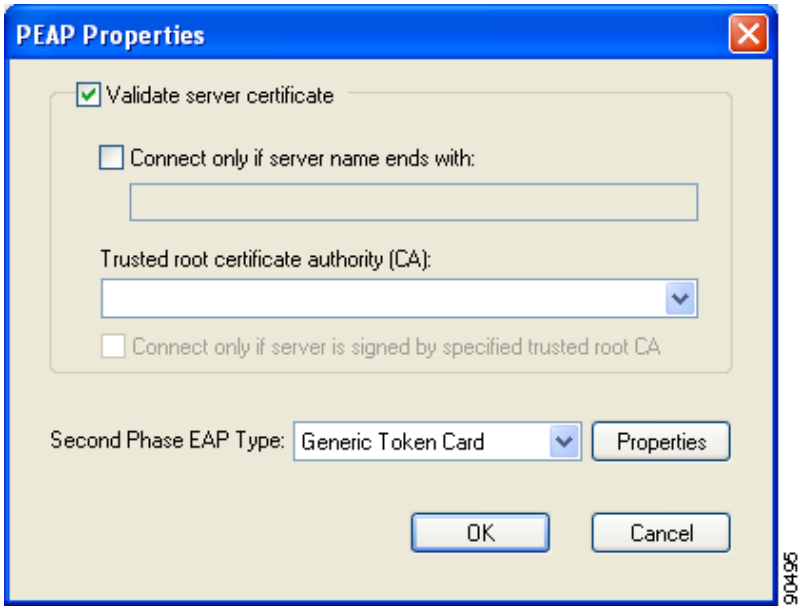
Step 9 The EAP authentication process begins automatically, and the client adapter should EAP authenticate using your Windows credentials. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection.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

Enabling PEAP (EAP-GTC)

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

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

Figure E-8 PEAP Properties Window



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

Step 3 If you want to specify the name of the server to connect to, check the **Connect only if server name ends with** check box and enter the appropriate server name suffix in the field below.

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

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

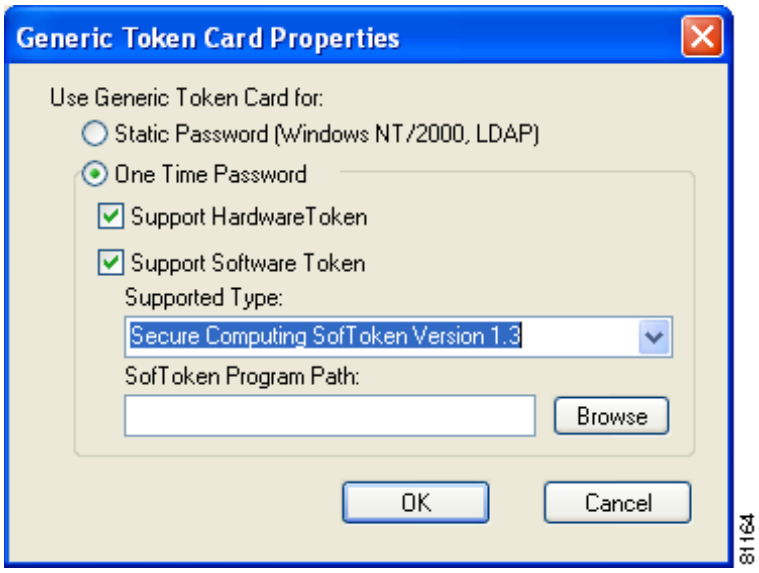
Step 4 Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority (CA) field. If necessary, click the arrow on the drop-down menu and choose the appropriate name.

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

Step 5 Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.

Step 6 Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties window appears (see Figure E-9).

Figure E-9 Generic Token Card Properties Window



Step 7 Choose either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.

Step 8 Perform one of the following:

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

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

Step 9 Click **OK** in each window to save your settings. The configuration is complete.

Step 10 Refer to Chapter 6 of the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* (OL-1394-07 or later) for instructions on authenticating using PEAP (EAP-GTC).

Associating to an Access Point Using Windows XP

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

Viewing the Current Status of Your Client Adapter

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

Figure E-10 Wireless Network Connection Status Window