# 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, page E-2
- Configuring the Client Adapter, page E-5
- Enabling Wi-Fi Multimedia, page E-19
- Associating to an Access Point Using Windows XP, page E-21
- Viewing the Current Status of Your Client Adapter, page E-21

# Overview

This appendix provides instructions for minimally configuring the client adapter through Windows XP (instead of through ACU) as well as for enabling one of 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, the 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.

Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter, and they are lost when power to the adapter is removed or the Windows device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows device is rebooted. This is 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 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.

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

- **EAP-TLS**—This authentication type is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data.

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

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

- **Protected EAP** (or **PEAP**)—PEAP 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 is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. If your network uses an OTP user database, PEAP 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 requires you to enter your username, password, and domain name in order to start the authentication process.

  RADIUS servers that support PEAP authentication include Cisco Secure ACS version 3.1 or later and Cisco Access Registrar version 3.5 or later.

  **Note** To use PEAP authentication, you must install the PEAP supplicant during installation or Windows XP Service Pack 1. This Service Pack includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU after Windows XP Service Pack 1. Otherwise, Cisco's PEAP supplicant is overwritten by Microsoft's PEAP supplicant.

- **EAP-SIM**—EAP-SIM authentication is designed for use in public wireless LANs and requires clients equipped with PCSC-compliant smartcard readers. The EAP-SIM supplicant included in the Install Wizard file supports only Gemplus SIM+ cards; however, an updated supplicant is available that supports standard GSM-SIM cards as well as more recent versions of the EAP-SIM protocol. The new supplicant is available for download from Cisco.com at the following URL:

  http://www.cisco.com/cgi-bin/tablebuild.pl/access-registrar-encrypted

  Please note that the above requirements are necessary but not sufficient to successfully perform EAP-SIM authentication. Typically, you are also required to enter into a service contract with a WLAN service provider, who must support EAP-SIM authentication in its network. Also, while your PCSC smartcard reader may be able to read standard GSM-SIM cards or chips, EAP-SIM authentication usually requires your GSM cell phone account to be provisioned for WLAN service by your service provider.

  EAP-SIM is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-SIM requires you to enter a user verification code, or *PIN*, for communication with the SIM card. You can choose to have the PIN stored in your computer or to be prompted to enter it after a reboot or prior to every authentication attempt.

RADIUS servers that support EAP-SIM include Cisco Access Registrar version 3.0 or later.

When you enable Require EAP on your access point and configure your client adapter for EAP-TLS, PEAP, or EAP-SIM 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), certificate (EAP-TLS), or internal key stored on the SIM card and in the service provider's Authentication Center (EAP-SIM) being the shared secret for authentication. The password or internal key 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/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm

## Wi-Fi Protected Access (WPA)

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

WPA supports two mutually exclusive key management types: WPA and WPA-Pre-shared key (WPA-PSK). 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). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

Windows XP Service Pack 1 and Microsoft support patch 815485 must be installed in order to use WPA. They can be downloaded from the following URLs:

- Service Pack 1: http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp
- 815485 support patch: http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en

Only 350 series and CB20A cards that are running EAP authentication can be used with WPA. WPA must also be enabled on the access point.

**Note** 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 these steps to configure your client adapter using Windows XP.

**Note** If you installed ACU but intend to use Windows XP to configure the client adapter, open ACU and make sure the **Use Another Application to Configure My Wireless Settings** option is selected on the Select Profile screen.

**Note** These instructions assume you are using the following:
- Windows XP Service Pack 1 and Microsoft support patch 815485
- Windows XP's classic view rather than its category view

If you do not use Service Pack 1 and the 815485 support patch, the screens you see will look different than those shown in this section. Refer to version OL-1394-06 of this manual if you need instructions on configuring a client adapter through Windows XP without these software upgrades.

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

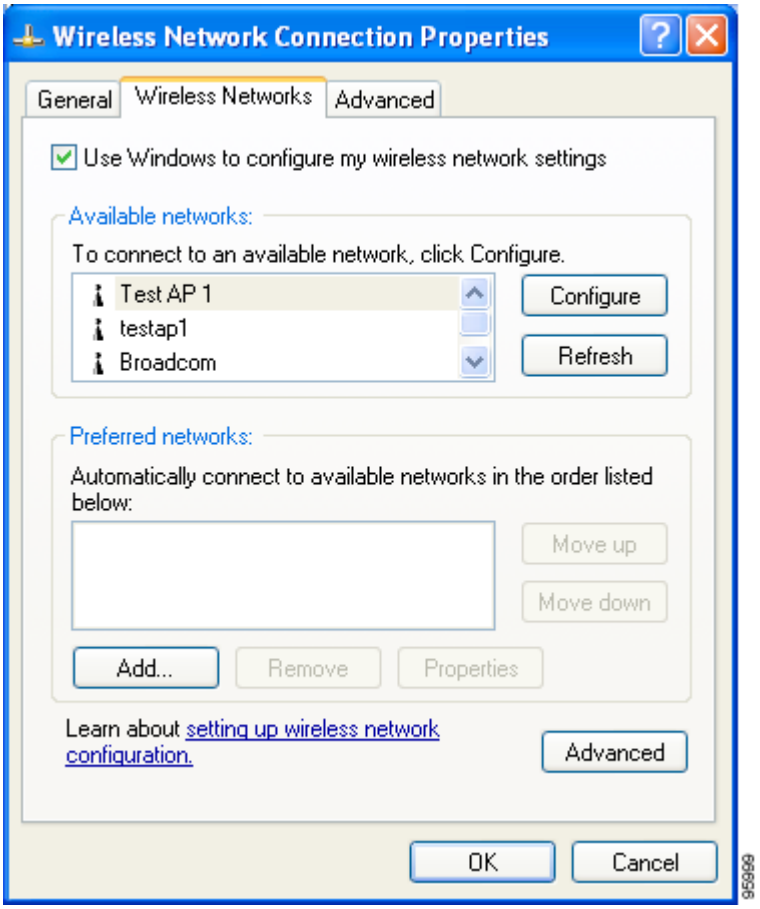
**Step 2** Double-click **My Computer**, **Control Panel**, and **Network Connections**.

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

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

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

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



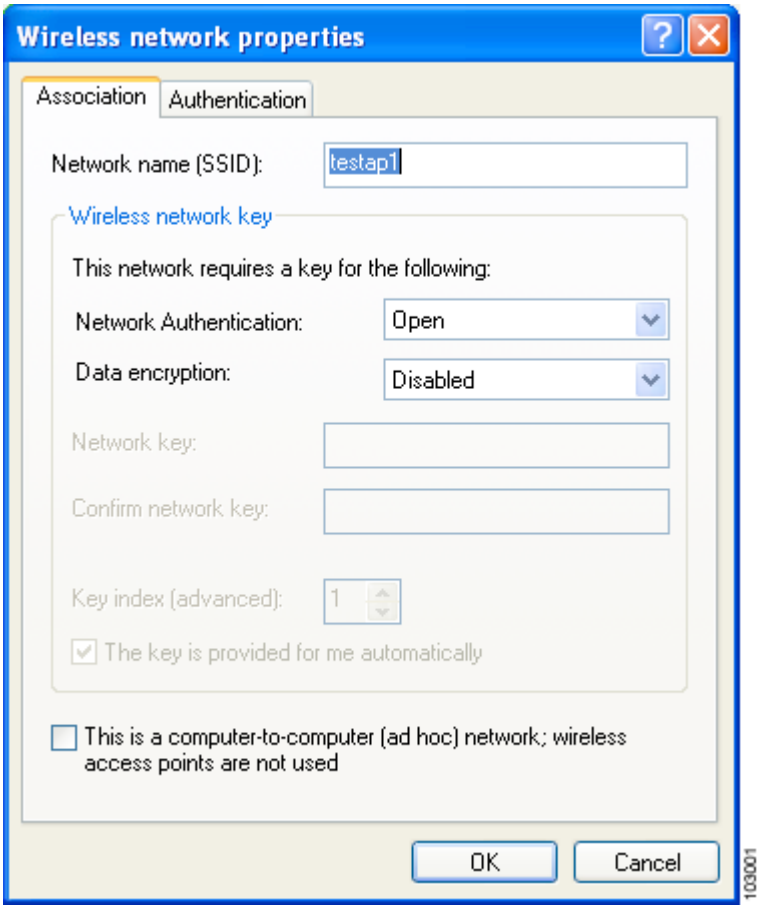

**Step 6** Make sure that the **Use Windows to configure my wireless network settings** check box is checked.

**Step 7** Click 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 screen appears (see Figure E-2).

*Figure E-2 Wireless Network Properties Screen (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 screen 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. This option is recommended if you want to use static WEP or EAP authentication without WPA.
- **Shared**—Enables your client adapter to 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** 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.
- **WPA-None**—Enables WPA for your client adapter when the client is set for ad hoc mode.

**Note** Refer to the "Wi-Fi Protected Access (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.

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

**Note** If you are planning to use EAP-TLS, PEAP, or EAP-SIM 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:** 5A58313533355459554933353 4 (hexadecimal) or ZX1535TYUI354 (ASCII)

  **Note** You must enter hexadecimal characters for 5-GHz client adapters if these adapters will be used with Cisco Aironet 1200 Series 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 or WPA-None, obtain the pre-shared 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 pre-shared key:

- Pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

**Note** You must enter hexadecimal characters for 5-GHz client adapters if these adapters will be used with Cisco Aironet 1200 Series Access Points.

- Your client adapter's pre-shared key must match the pre-shared key used by the access point (in infrastructure mode) or clients (in ad hoc mode) 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, PEAP, or EAP-SIM, 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:

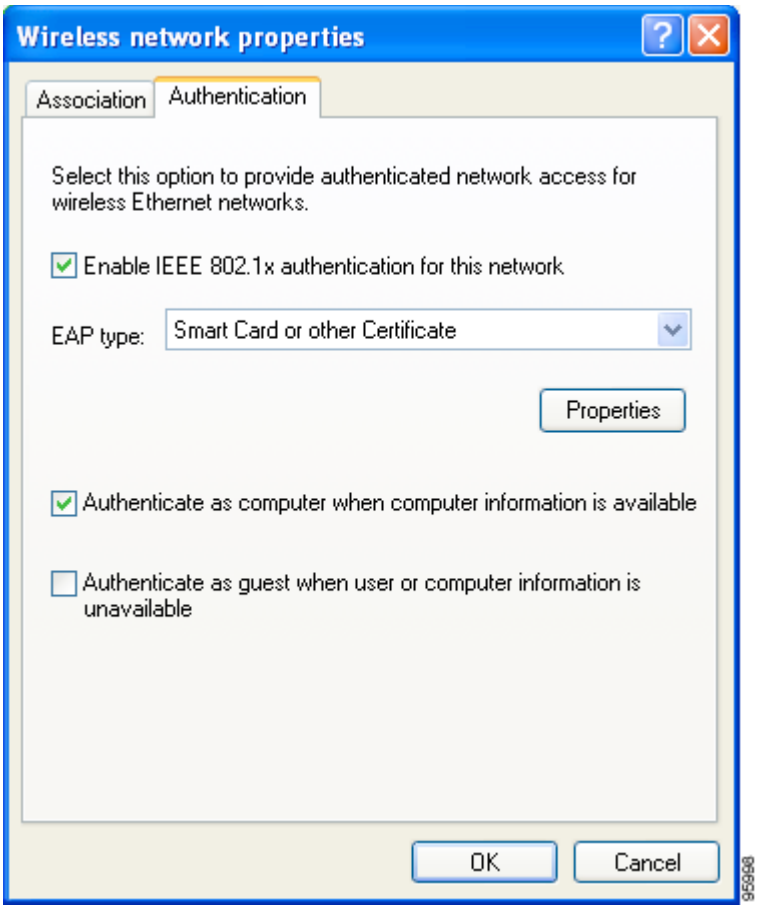
- If you are planning to use EAP-TLS authentication, follow the instructions in the "Enabling EAP-TLS Authentication" section below.
- If you are planning to use PEAP authentication, follow the instructions in the "Enabling PEAP Authentication" section on page E-13.
- If you are planning to use EAP-SIM authentication, follow the instructions in the "Enabling EAP-SIM Authentication" section on page E-16.

# Enabling EAP-TLS Authentication

Follow these steps 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 screen. The following screen appears (see Figure E-3).

***Figure E-3 Wireless Network Properties Screen (Authentication Tab)***

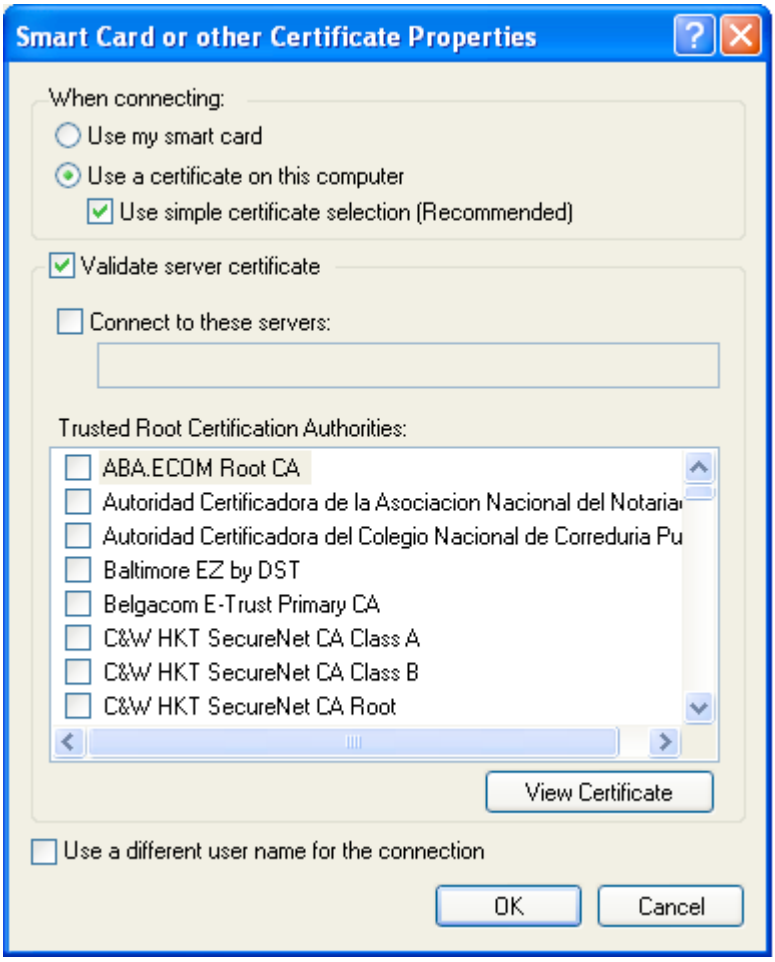



**Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA or WPA-PSK on the Association screen.

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

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

*Figure E-4 Smart Card or Other Certificate Properties Screen*




**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** three times 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.

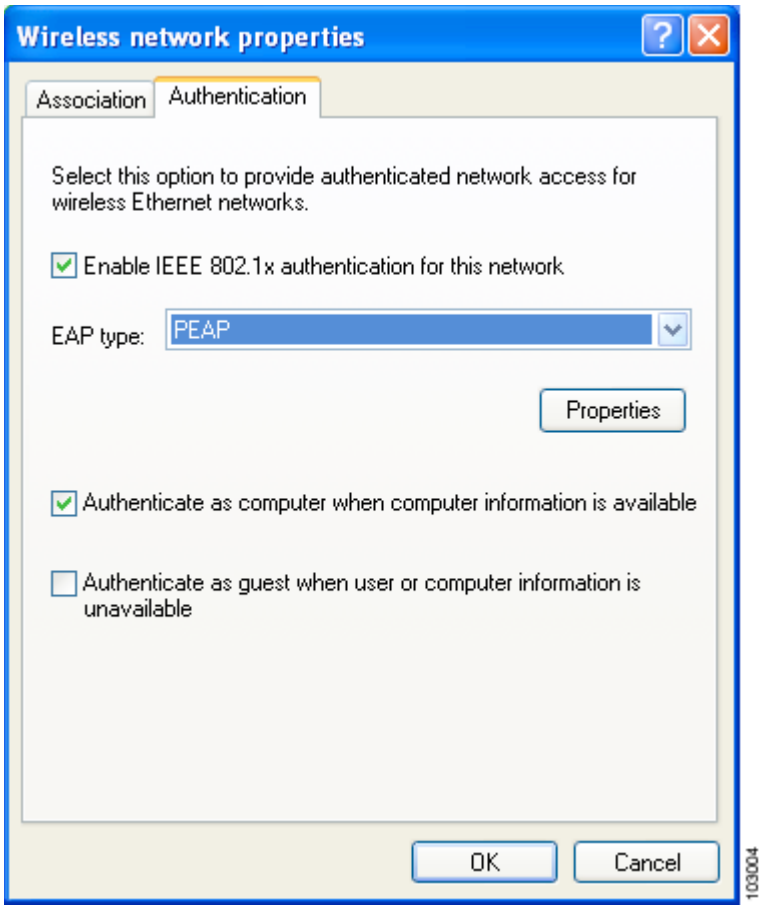
**Step 14** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads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

# Enabling PEAP Authentication

Follow these steps 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 screen. The following screen appears (see Figure E-5).

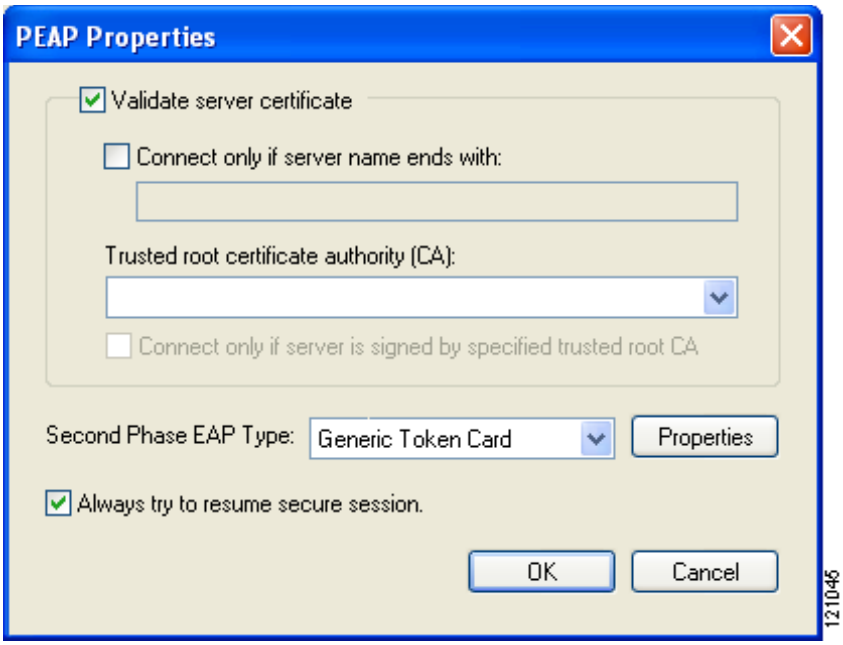
***Figure E-5 Wireless Network Properties Screen (Authentication Tab)***




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

**Step 3** For EAP type, choose **PEAP**. Click **Properties**. The PEAP Properties screen appears (see Figure E-6).

*Figure E-6 PEAP Properties Screen*




**Step 4** Check the **Validate server certificate** check box if server certificate validation is required (recommended).

**Step 5** 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 6** 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 7** 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.

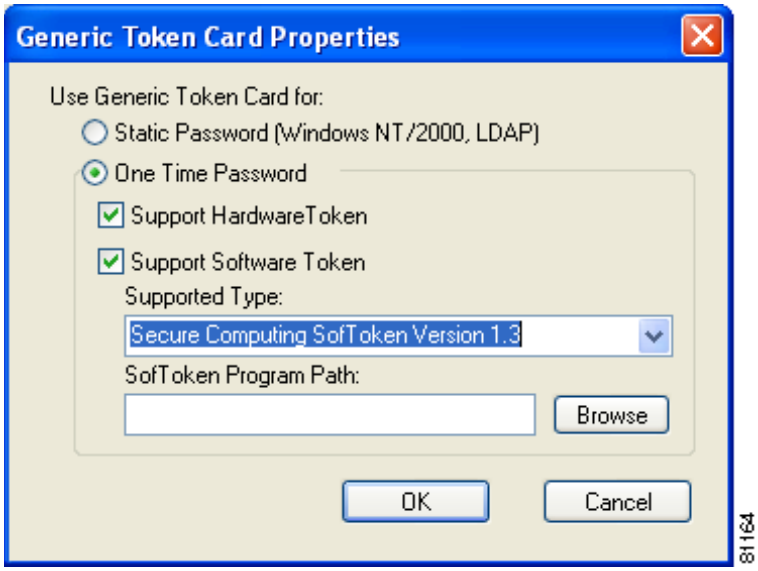
**Step 8** Perform one of the following:

- 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 screen 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 9** Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties screen appears (see Figure E-7).

***Figure E-7 Generic Token Card Properties Screen***




**Step 10** Choose either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.

**Step 11** Perform one of the following:

- If you selected the **Static Password (Windows NT/2000, LDAP)** option in Step 10, go to Step 12.
- If you selected the **One Time Password** option in Step 10, 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 1.3, Secure Computing SofToken II 2.0, or RSA SecurID Software Token v 2.5), and if Secure Computing SofToken Version 1.3 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 1.3 is selected.

**Step 12** Click **OK** four times to save your settings. The configuration is complete.

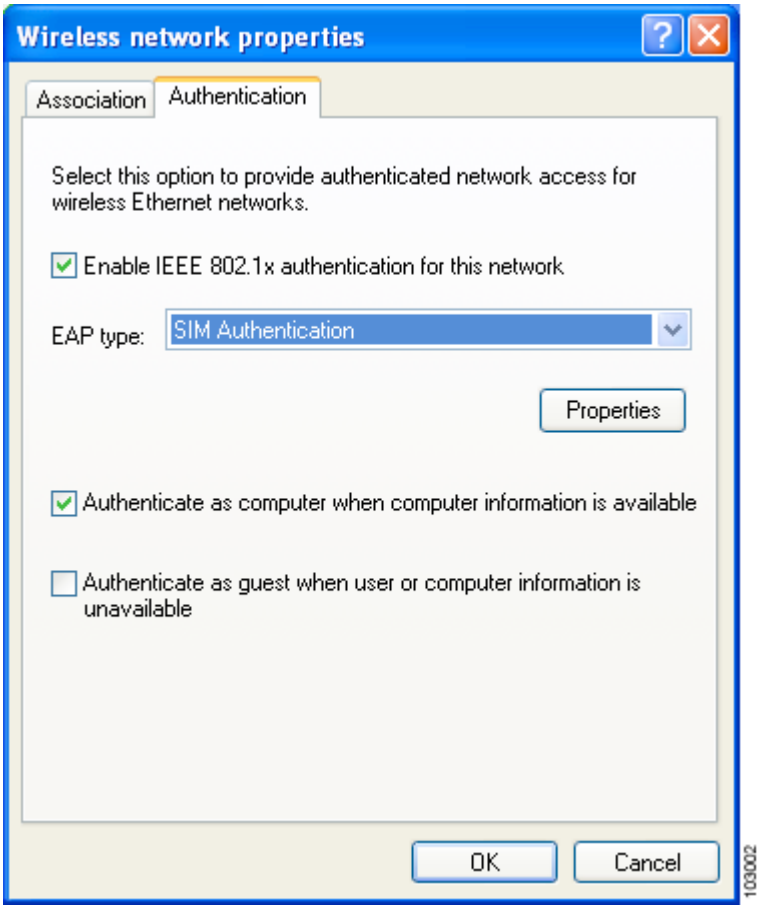
**Step 13** Refer to the "Using PEAP" section on page 6-23 for instructions on authenticating using PEAP.

# Enabling EAP-SIM Authentication

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

**Step 1** Click the **Authentication** tab on the Wireless Network Properties screen. The following screen appears (see Figure E-8).

*Figure E-8 Wireless Network Properties Screen (Authentication Tab)*

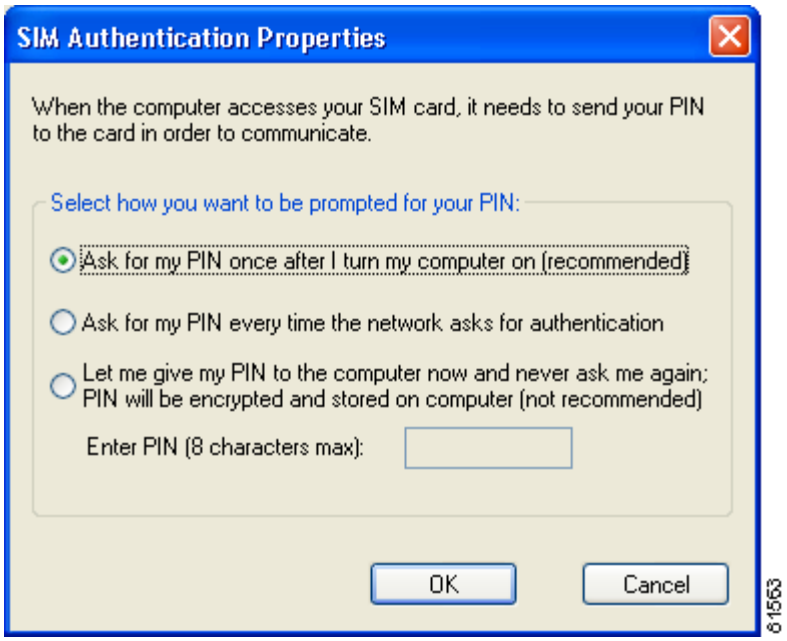



**Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA or WPA-PSK on the Association screen.

**Step 3** For EAP type, choose **SIM Authentication**.

**Step 4** Click **Properties**. The SIM Authentication Properties screen appears (see Figure E-9).

*Figure E-9 SIM Authentication Properties Screen*




**Step 5** To access any resources (data or commands) on the SIM, the EAP-SIM supplicant must provide a valid PIN to the SIM card, which must match the PIN stored on the SIM. Choose one of the following options to specify how the EAP-SIM supplicant should handle the SIM card's PIN:

- **Ask for my PIN once after I turn my computer on (recommended)**—The software does not permanently store the PIN. It prompts you for the PIN once, on the first authentication of every session, where a *session* is defined as the time between power-up and shutdown or reboot.
- **Ask for my PIN every time the network asks for authentication**—The software never stores the PIN; it prompts you for the PIN every time an EAP-SIM authentication is performed. This option is not recommended if your client will be roaming between access points or if session timeouts are implemented (such as for accounting and security purposes).
- **Let me give my PIN to the computer now and never ask me again; PIN will be encrypted and stored on computer (not recommended)**—You need to enter the PIN only once, in the Enter PIN edit box below this option. The software stores the PIN in the registry and retrieves it from there when required. If you choose this option, you must enter the PIN now. The PIN is validated when an authentication attempt is made.

**Note** This option is not recommended because it enables others to use the SIM without knowing the PIN.

**Step 6** Click **OK** three times to save your settings. The configuration is complete.

If you chose to store the PIN in the computer's registry, the EAP authentication process begins automatically, and the client adapter should EAP authenticate and use the saved PIN to access the SIM card.

**Note** If the stored PIN is wrong and therefore rejected by the SIM, the EAP-SIM supplicant temporarily changes the prompt mode to the default setting (Ask for my PIN once after I turn my computer on) in order to prevent the SIM from locking up. Unless changed manually, this setting stays in effect until your computer is powered off. Change your stored PIN on the SIM Authentication Properties screen.

If you chose to be prompted for the PIN after a power-up or reboot or at every authentication request, a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network. Click the message, enter your PIN, and click **OK**. The client adapter should now EAP authenticate.

**Step 7** 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*.

**Note** ACU and the Windows Wireless Network Connection icon in the Windows XP system tray may indicate a connection status when authentication is still in the pending state or the authentication server fails to respond.

# Enabling Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing. QoS is an access point feature that enables networking professionals to provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. Implementing QoS in a wireless LAN makes network performance more predictable and bandwidth usage more effective.

Cisco recommends that you enable WMM if your computer is running a time-sensitive application for QoS-aware clients such as voice or video (for example, Cisco IP SoftPhone).

QoS and WMM must be enabled on the access point to which the client will associate. These features are supported on the access point in Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling these features.

WMM is supported automatically in client adapter firmware version 5.60.08, PC/LM/PCI card driver version 8.6, and mini PCI/CB20A card driver version 3.9, which are included in Install Wizard version 1.5 or later. However, you must enable the Windows QoS Packet Scheduler to ensure WMM support.

Follow these steps to enable the QoS Packet Scheduler on a computer running Windows XP.

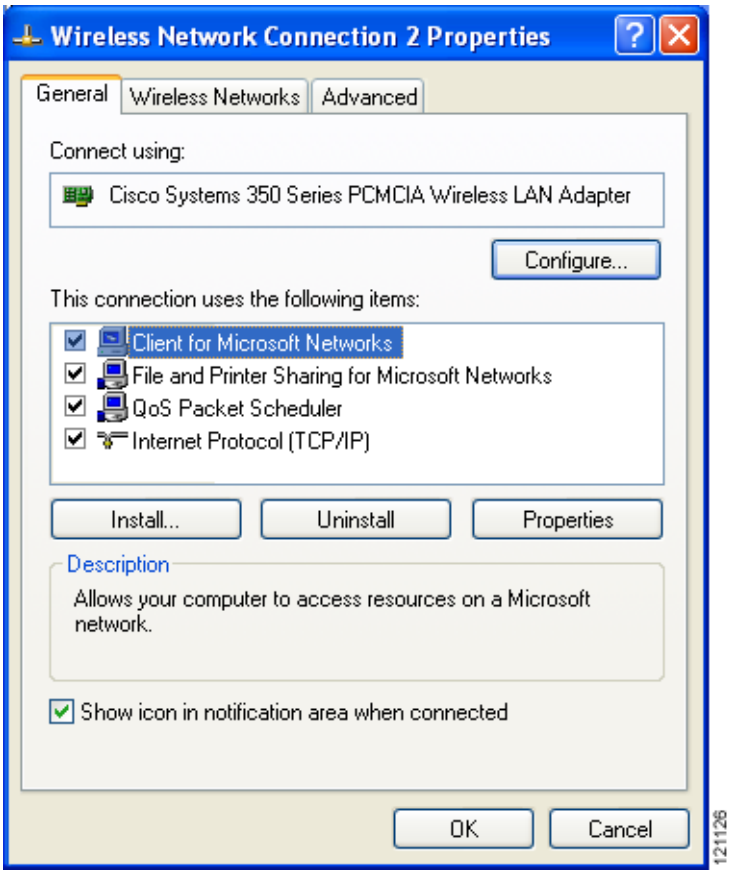
**Step 1** Double-click **Control Panel**.

**Step 2** Click **Network Connections**.

**Step 3** Right-click your wireless network connection.

**Step 4** Click **Properties**. The Wireless Network Connection Properties screen appears (see Figure E-10).

***Figure E-10 Wireless Network Connection Properties Screen***




**Step 5** Check the **QoS Packet Scheduler** check box, which appears in the list of items that this connection uses.

**Step 6** Click **OK**.

# 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 screen appears (see Figure E-11).

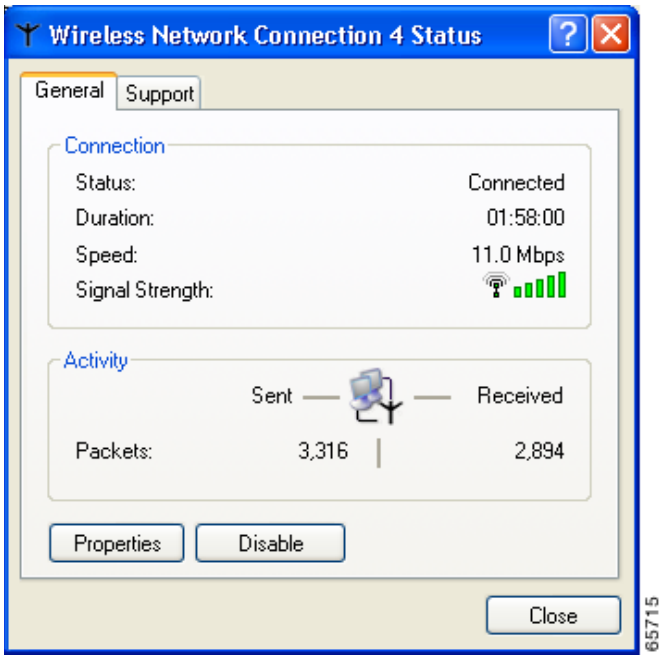



***Figure E-11 Wireless Network Connection Status Screen***