CHAPTER 2

Configuring Wireless Profiles

This chapter explains how to use the Microsoft Vista Network and Sharing Center to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

- Overview of Wireless Profiles, page 2-2
- Accessing Microsoft Vista Network and Sharing Center, page 2-2
- Creating a New Profile and Configuring Basic Settings, page 2-3
- Accessing a Profile That Was Created Previously, page 2-12
- Viewing and Changing the Settings of a Profile, page 2-13

Overview of Wireless Profiles

A wireless profile is a set of of configuration parameters that you (or your network administrator) can create and manage in the Microsoft Vista user interface. You can connect to a wireless network with the profile, which includes the wireless network name, the network security type, the network encryption type, and other feature configurations.

You can create several different profiles that enable you to connect to wireless networks in different locations. For example, you might want to create and manage profiles that allow you to use your client adapter at the office, at home, and in public areas, such as airport terminals. After the profiles are created, you can switch between them without having to configure your client adapter each time you move to a new location.

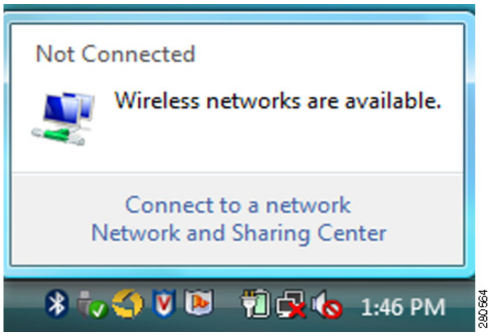
Accessing Microsoft Vista Network and Sharing Center

To create and manage wireless profiles, you must access the Microsoft Vista Network and Sharing Center.

To access the Network and Sharing Center window, follow these steps:

Step 1 Double-click the networking icon (two computer monitors) in the system tray at the bottom right corner of the screen. A small dialog box appears (see Figure 2-1).

Figure 2-1 Networking Icon in System Tray

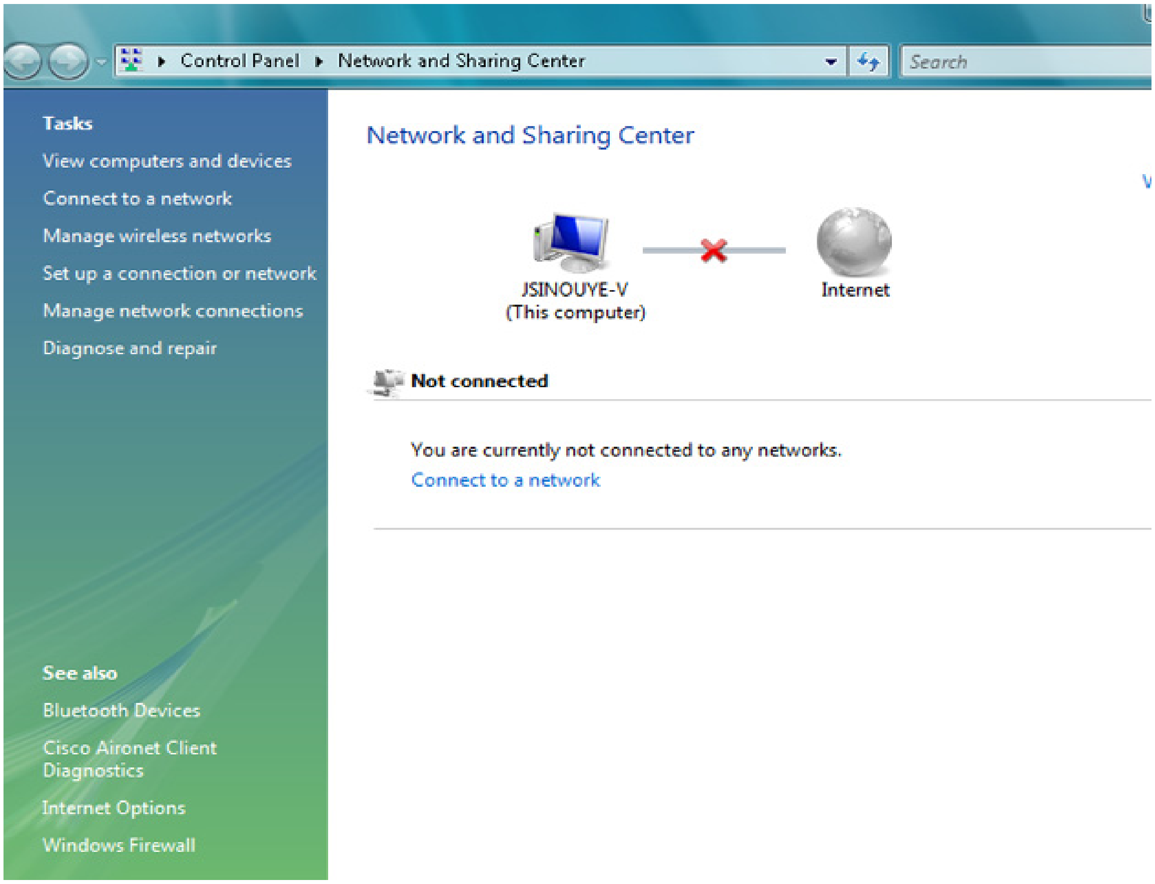


Not Connected

Wireless networks are available.

Step 2 Click **Network and Sharing Center**. The Network and Sharing window appears (see Figure 2-2).

Figure 2-2 Network and Sharing Center Window



You are currently not connected to any networks.

Step 3 To set up a wireless profile, click **Set up a connection or network** in the Tasks area.

Note You can also access the Network and Sharing Center by choosing **Start > Control Panel > Network and Sharing Center**.

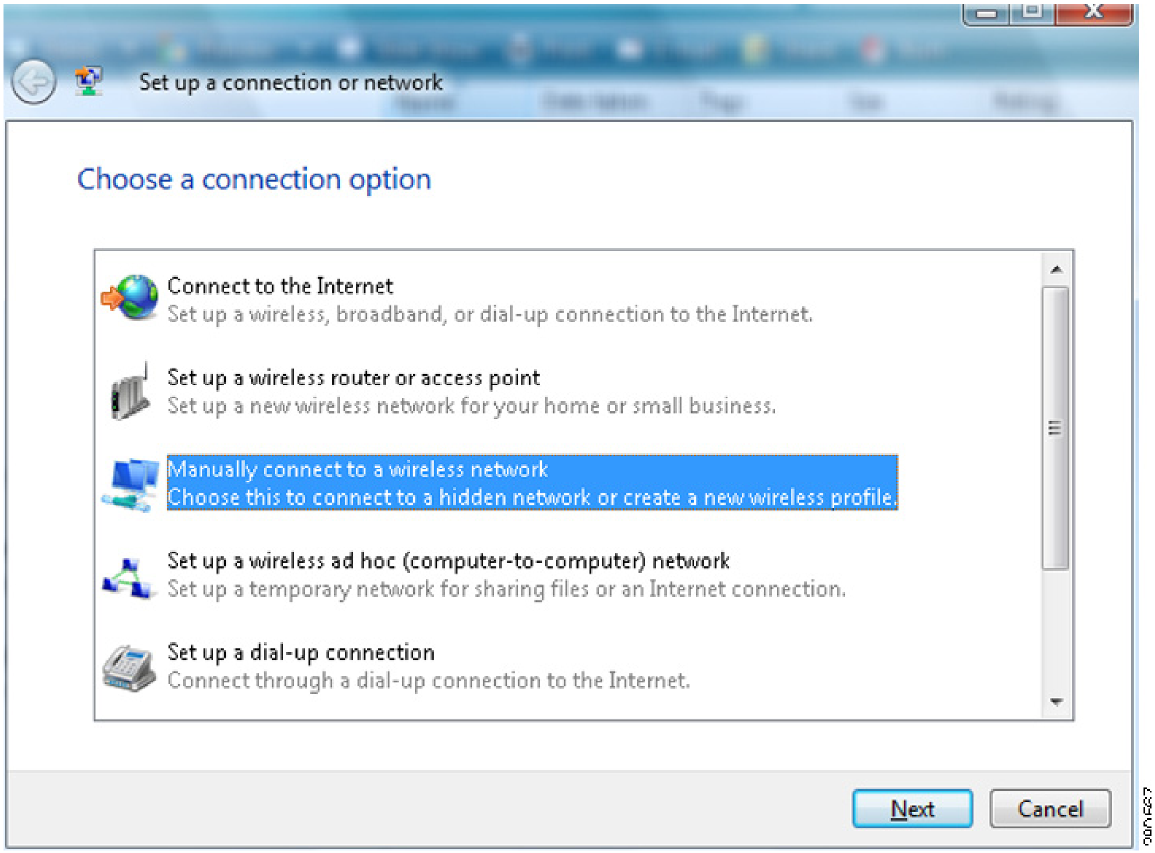
Creating a New Profile and Configuring Basic Settings

To create a wireless profile, follow these steps:

Step 1 Open the Network and Sharing Center window (see the "Accessing Microsoft Vista Network and Sharing Center" section on page 2-2).

Step 2 Click **Set up a connection or network** in the Tasks area. The Set up a connection or network dialog box appears (see Figure 2-3).

Figure 2-3 Set up a connection or network Dialog Box



Set up a connection or network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a wireless router or access point
Set up a new wireless network for your home or small business.

Manually connect to a wireless network
Choose this to connect to a hidden network or create a new wireless profile.

Set up a wireless ad hoc (computer-to-computer) network
Set up a temporary network for sharing files or an Internet connection.

Set up a dial-up connection
Connect through a dial-up connection to the Internet.

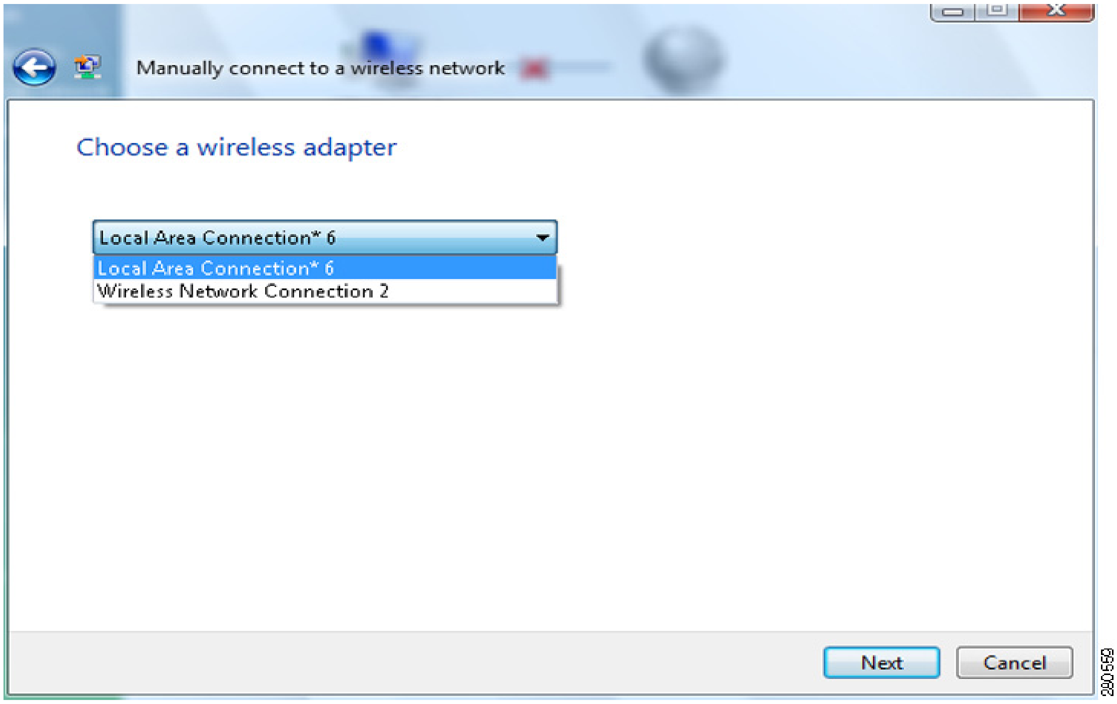
Step 3 In the Choose a connection option area, click **Manually connect to a wireless network**.

Step 4 Click **Next**. A Manually connect to a wireless network dialog box appears (see Figure 2-4.)

Step 5 From the Choose a wireless adapter drop-down list, choose the option for the Cisco Aironet 802.11a/b/g Wireless Adapter (see Figure 2-4).

Note Client adapters might not be easy to identify in the Choose a wireless adapter drop-down list because the adapters might be generically named (for example, Wireless Network Connection or Wireless Network Connection 2). If you have multiple client adapters on your device, choose **Network and Sharing Center > Manage network connections**. In the Views drop-down list, choose **Details** to see which generic name corresponds with which client adapter. When you view the details of available network connections, the client adapter is identified in the Device Name column.

Figure 2-4 Manually connect to a wireless network Dialog Box—Choose a wireless adapter

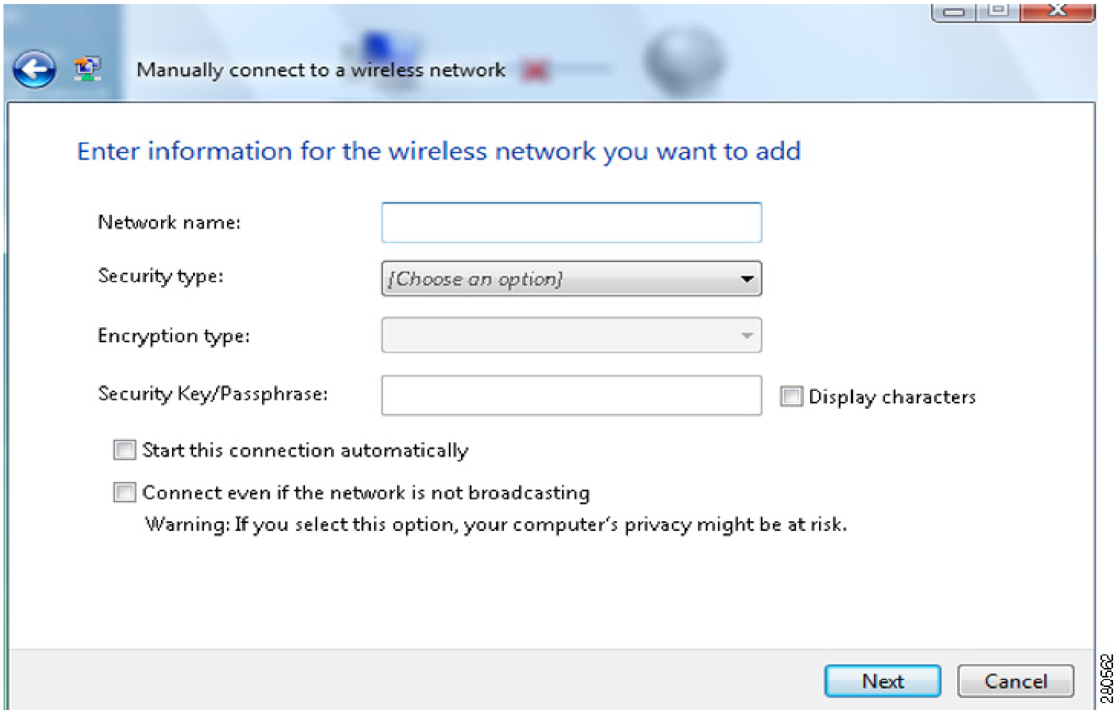


Choose a wireless adapter

Local Area Connection* 6
Local Area Connection* 6
Wireless Network Connection 2

Step 6 Click **Next**. Another Manually connect to a wireless network dialog box appears (see Figure 2-5).

Figure 2-5 Manually connect to a wireless network Dialog Box—Enter information for the wireless network you want to add



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: [Choose an option]

Encryption type:

Security Key/Passphrase: □ Display characters

□ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Step 7 In this dialog box, enter information for the wireless network that you want to add.Table 2-1 lists and describes general settings for the profile. Follow the instructions in the table to configure these settings.

Table 2-1 Profile Management General Settings

Setting	What to Enter
Network name	Enter the service set identifier (SSID). The network name and the SSID are the same. **Range:** The network consists of 1 to 32 case-sensitive characters. **Default:** A blank field
Security type	From the Security type drop-down list, choose the method that is used to secure a connection to the wireless network. The choices are the following: • No authentication (Open)—Open system authentication with no encryption • WEP (also called Shared)—Open system authentication with Wired Equivalent Privacy (WEP) • WPA2-Personal—Wi-Fi Protected Access 2 (WPA2) authentication with a preshared key (designed for networks without a RADIUS infrastructure) • WPA-Personal—WPA with a preshared key (designed for networks without a RADIUS infrastructure) • WPA2-Enterprise—802.1X authentication (designed for medium and large infrastructure mode networks) • WPA-Enterprise—802.1X authentication (designed for medium and large infrastructure mode networks) • 802.1x—802.1X authentication with WEP (also known as dynamic WEP). • CCKM—Cisco Centralized Key Management For more information about these security types, see the "Security and Encryption Types" section on page 2-10. **Default:** None. You must choose a security type to create a wireless profile.

Table 2-1 Profile Management General Settings (continued)

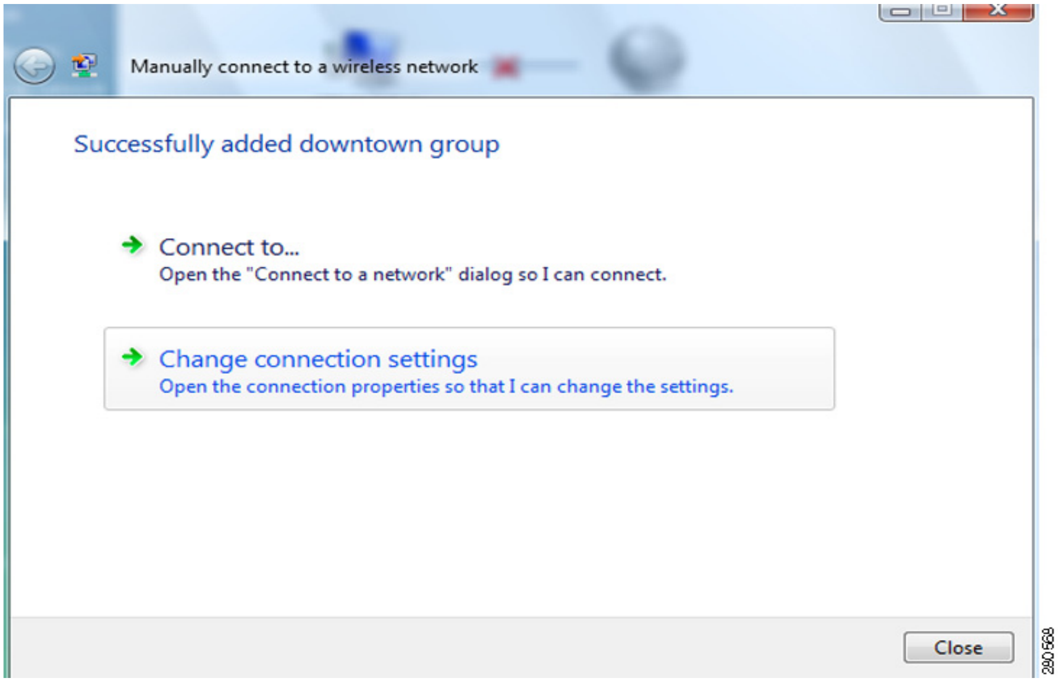
Setting	What to Enter
Encryption type	Encryption choices are determined by the security type that you choose. From the Encryption type drop-down list, choose an available method. The choices are the following: • If you choose No authentication (Open), your encryption choice is None. • If you choose WEP, your only encryption choice is WEP. • If you choose WPA2-Personal, you can choose AES or TKIP. • If you choose WPA-Personal, you can choose AES or TKIP. • If you choose WPA2-Enterprise, your encryption choice is AES, TKIP, AES (MFP), or TKIP (MFP). • If you choose WPA-Enterprise, your encryption choice is AES or TKIP. • If you choose 802.1x, your only encryption choice is WEP. • If you choose CCKM, your encryption choices are WEP, AES, and TKIP. For more information about these encryption types, see the "Security and Encryption Types" section on page 2-10. **Default:** The default that appear in the Encryption type drop-down list is determined by what you selected in the Security type drop-down list.
Security Key/Passphrase	• If you choose No authentication (Open), a Security Key/Passphrase is not necessary. • If you choose the WEP security type, enter the WEP key. • If you choose the WPA2-Personal security type, enter the WPA2 preshared key. • If you choose the WPA-Personal security type, enter the WPA preshared key. • For the WPA2-Enterprise and WPA-Enterprise security types, see Chapter 3, "Configuring EAP Types." The enterprise network EAP type determines the credentials that the client adapter must use for authentication. • If you choose the 802.1x security type, a Security Key/Passphrase is not necessary. **Note** Contact the wireless network administrator for the network WEP key, the WPA2-Personal preshared key, or the WPA-Personal preshared key.
Display characters	Check this check box if you want to view the characters that you enter into the Security Key/Passphrase field. If you do not check this check box, the key or passphrase that you enter appears as black dots. **Default:** Not checked.

Table 2-1 Profile Management General Settings (continued)

Setting	What to Enter
Start this connection automatically	Check this check box if you want the device to connect automatically whenever the wireless network is in range. If you do not check this check box, you must manually connect to this wireless network from the Connect to a network dialog box, which you can access through the Network and Sharing Center. **Default:** For the No authentication (Open) security type, this check box is unchecked. For all other security types, this check box is checked.
Connect even if the network is not broadcasting	Check this check box if you want the device to attempt to connect even if the wireless network is not broadcasting its name. **Default**: Not checked.

Step 8 After you enter all required settings, click **Next**. Another Manually connect to a wireless network dialog box appears (see Figure 2-6).

Figure 2-6 Manually connect to a wireless network Dialog Box—Successfully added <network name>



Manually connect to a wireless network

Successfully added downtown group

Connect to...
Open the "Connect to a network" dialog so I can connect.

Change connection settings
Open the connection properties so that I can change the settings.

Step 9 Click **Connect to** to connect to a wireless network, including the one for which you have created a profile. Or click **Change connection settings** to change the profile settings. See the "Viewing and Changing the Settings of a Profile" section on page 2-13 for more information.

Security and Encryption Types

The dialog box in Figure 2-5 includes the settings that allow you to configure how the client adapter associates to an access point, authenticates to a wireless network, and encrypts and decrypts data. The following sections provide explanations of options that are available in the Security type drop-down list, the Encryption type drop-down list, and the Security Key/Passphrase field of this dialog box.

WEP (Shared) Security with Static WEP Keys

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 client adapter. Static WEP keys are either 40 or 128 bits in length. 128-bit WEP keys offer more security than 40-bit WEP keys.

Each profile can be assigned a static WEP keys. If the 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 the static WEP key each time the client adapter is inserted or the Windows device is rebooted because the key is stored (in an encrypted format for security reasons) in the Windows profile store.

You can obtain a static WEP key from your network administrator.

Note WEP encryption is not considered safe enough for today’s wireless networks. We do not recommend that you use it in enterprise wireless networks.

WPA and WPA2

Wi-Fi Protected Access (WPA) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA is compatible with the IEEE 802.11i standard but was implemented prior to the standard’s ratification; WPA2 is the Wi-Fi Alliance’s implementation of the ratified IEEE 802.11i standard.

WPA and WPA2 can use Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection or the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA and WPA2 use 802.1X for authenticated key management.

Both WPA and WPA2 support two mutually exclusive key management types: WPA/WPA2 and WPA/WPA2 passphrase (also known as WPA pre-shared key or WPA-PSK). Using WPA or WPA2, 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 or WPA2 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.

- WPA2-Personal—WPA2 authentication with a preshared key. WPA2-Personal is suitable for environments without a Remote Authentication Dial-In User Service (RADIUS) infrastructure (for example, a small office or home office network). WPA2-Personal supports the use of a preshared key (PSK).Obtain the preshared key from your system administrator. When you choose WPA2-Personal as your security type, your encryption type is TKIP or AES.
- WPA-Personal—WPA with a preshared key. Like WPA2-Personal, WPA-Personal is suitable for environments without a RADIUS infrastructure. Obtain the preshared key from your system administrator. When you choose WPA-Personal as your security type, your encryption type is TKIP or AES.
- WPA2-Enterprise—WPA2-Enterprise requires authentication in two phases: the first is an open system authentication, and the second uses 802.1X with an Extensible Authentication Protocol (EAP) authentication method. See chapter Chapter 3, "Configuring EAP Types," for more information about supported EAP methods. When you choose WPA2-Enterprise as your security type, your encryption type is TKIP or AES.
- WPA-Enterprise—WPA-Enterprise also uses 802.1X authentication and is designed for medium and large infrastructure mode networks. See chapter for more information about supported EAP methods. When you choose WPA-Enterprise as you security type, your encryption type is TKIP or AES.

802.1X 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.

Dynamic WEP keys are created as part of the EAP authentication process. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

When you choose the 802.1X with WEP encryption, you can configure the profile to use five different authentication methods of dynamic WEP key creation:

- Smart Card or other certificate—for more information about smart cards and other certification authentication, go to the Microsoft site:

  http://technet2.microsoft.com/windowsserver/en/library/7c6b414a-80c7-4bc1-b952-6eca6585dff91033.mspx?mfr=true
- Protected EAP (PEAP)
- LEAP
- PEAP-GTC
- EAP-FAST

Note For more information about EAP authentication methods, see Chapter 3, "Configuring EAP Types."

CCKM Fast Secure Roaming

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require it to prevent delays and gaps in conversation. CCKM fast secure roaming is enabled automatically for CB21AG and PI21AG clients using WPA/WPA2/CCKM with LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2). However, this feature must be enabled on the access point.

During normal operation, EAP-enabled clients mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for CCKM fast secure roaming, EAP-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 Cisco client devices to roam from one access point to another typically in under 150 milliseconds (ms). CCKM fast secure 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.

Accessing a Profile That Was Created Previously

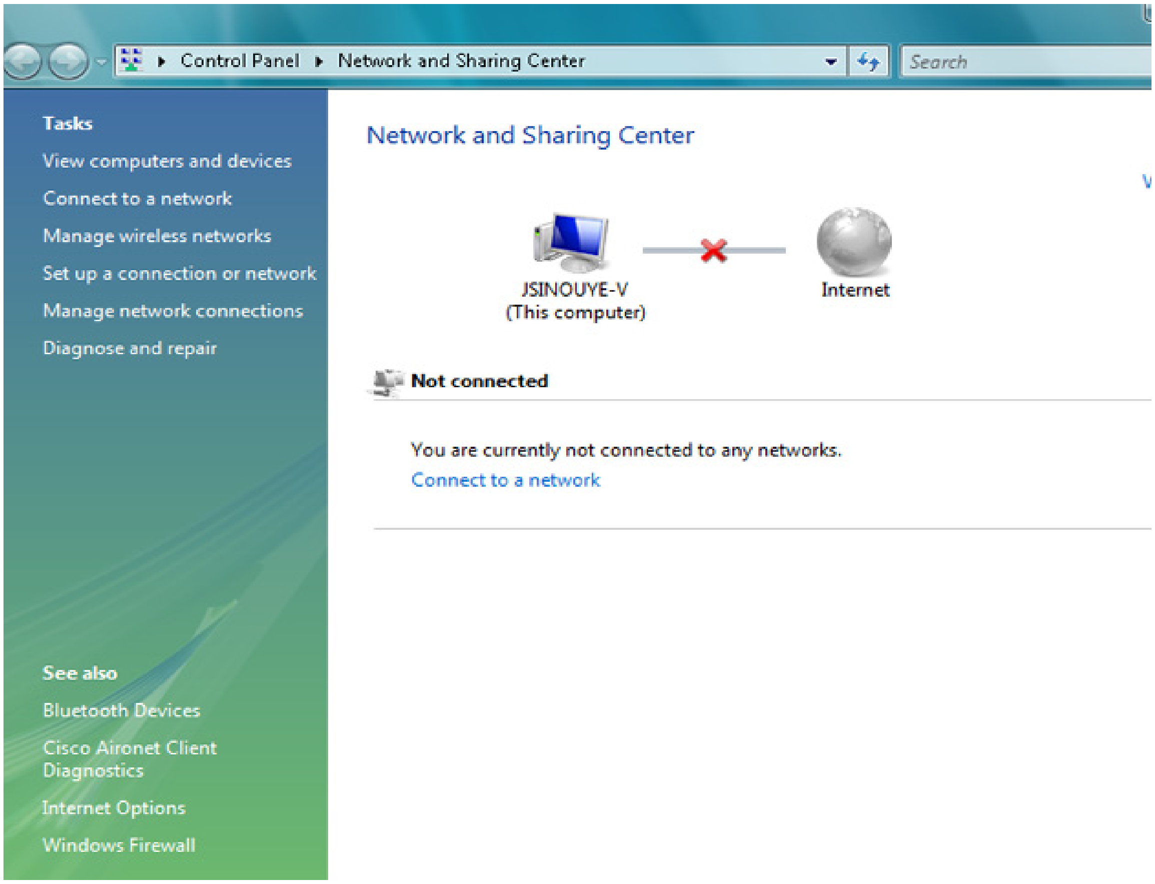
After you have created a profile and configured its basic settings (see the "Creating a New Profile and Configuring Basic Settings" section on page 2-3), you can change the settings by accessing the properties of the profile.

To access the profile, follow these steps:

Step 1 Open the Network and Sharing Center (see the "Accessing Microsoft Vista Network and Sharing Center" section on page 2-2).

Step 2 In the Network and Sharing window (see Figure 2-7), click **Manage wireless networks** in the Tasks area.

Figure 2-7 Network and Sharing Center Window



Control Panel ▸ Network and Sharing Center

Search

Tasks

View computers and devices

Connect to a network

Manage wireless networks

Set up a connection or network

Manage network connections

Diagnose and repair

See also

Bluetooth Devices

Cisco Aironet Client Diagnostics

Internet Options

Windows Firewall

Network and Sharing Center

JSINOUYE-V
(This computer)

Internet

Not connected

You are currently not connected to any networks.

Connect to a network

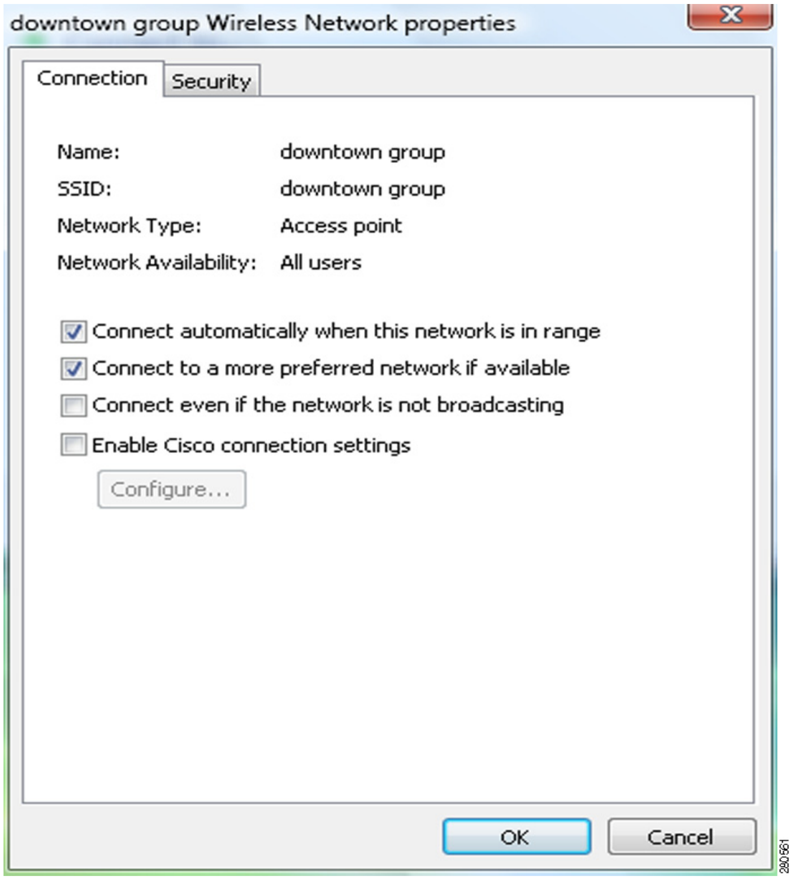
Step 3 In the Manage wireless networks window that appears, double-click the profile that contains the settings that you want to change. A Wireless Network properties dialog box appears (see Figure 2-8). See the "Viewing and Changing the Settings of a Profile" section on page 2-13 for information about modifying the profile that you have selected.

Viewing and Changing the Settings of a Profile

To access a profile whose settings you want to view or change, follow the procedure in the "Accessing a Profile That Was Created Previously" section on page 2-12. To view or change the settings of a profile, follow these steps:

Step 1 In the Connection tab of the Wireless Network properties dialog box (see Figure 2-8), view the wireless network's Name, SSID (service set identifier), Network Type (for example, Access point for an infrastructure-mode network), and the Network Availability (specifies the availability for types of users). You cannot change these settings in this dialog box.

Figure 2-8 Wireless Network properties Dialog Box—Connection Tab



downtown group Wireless Network properties

Name: downtown group

SSID: downtown group

Network Type: Access point

Network Availability: All users

☑ Connect automatically when this network is in range

☑ Connect to a more preferred network if available

☐ Connect even if the network is not broadcasting

☐ Enable Cisco connection settings

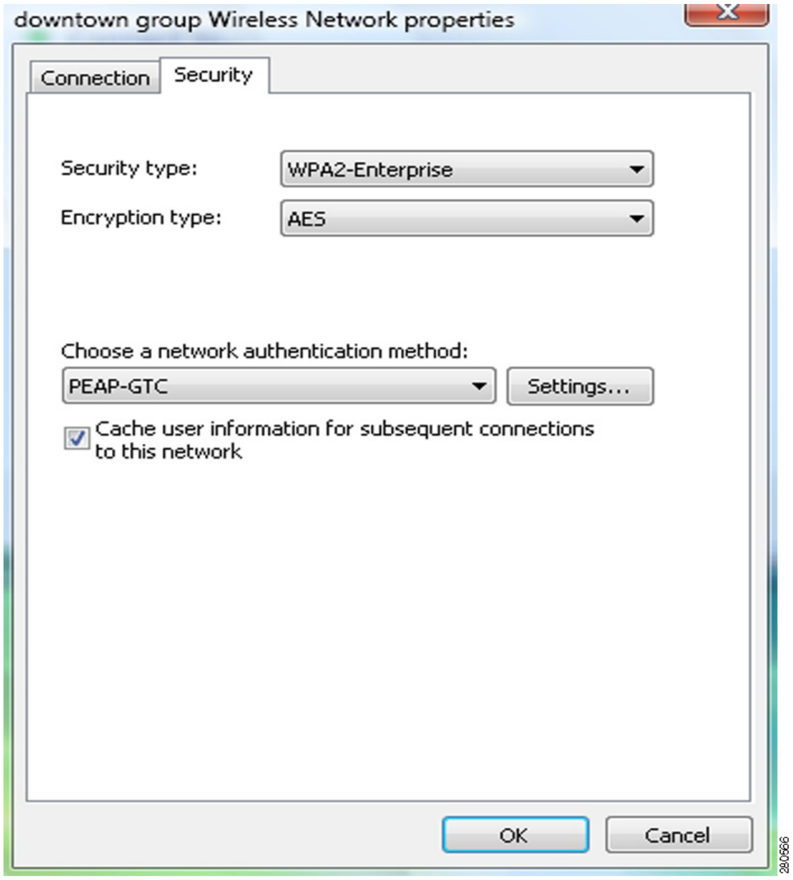
Step 2 In the Connection tab, check or uncheck the check boxes that are available. Table 2-2 lists and describes these check boxes. Follow the instructions in the table to configure these settings.

Table 2-2 Profile Management General Settings

Setting	What to Enter
Connect automatically when this network is in range	Check this check box if you want the device to connect automatically whenever the wireless network is in range. If you do not check this check box, you must manually connect to this wireless network from the Connect to a network dialog box, which you can access through the Network and Sharing Center. **Note** You configured this setting when you first created the wireless profile. See the Start this connection automatically check box in Table 2-1 on page 2-7.
Connect to a more preferred network if available.	Check this check box to connect to a wireless network that you prefer more than the wireless network specified in this profile. To designate the order in which your profiles connect when more than one network is available, Choose **Control Panel > Manage Wireless Networks**. You can order your wireless profiles in this window.
Connect even if the network is not broadcasting	Check this check box if you want the device to attempt to connect even if the wireless network is not broadcasting its name. **Note** You configured this setting when you first created the wireless profile. See the Connect even if the network is not broadcasting check box in Table 2-1 on page 2-7.
Enable Cisco connection settings	Check this check box to view, configure, and enable Radio Measurement and Advanced Roaming. When you check the **Enable Cisco connection settings** check box, the Configure button is no longer dimmed. Click on the **Configure** Button to open the Cisco Connection Settings dialog box. See the "Radio Measurement" section on page 2-18 and the "Advanced Roaming Setting" section on page 2-19 for more information about these Cisco connection settings.

Step 3 Click the **Security** tab to change security settings. The security settings on the Security tab appear (see Figure 2-9).

Figure 2-9 Wireless Network properties Dialog Box—Security Tab



downtown group Wireless Network properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: PEAP-GTC

☑ Cache user information for subsequent connections to this network

Step 4 In this dialog box, configure security settings that are available for this profile. Table 2-3 lists and describes security settings. Follow the instructions in the table to configure these settings.

Table 2-3 Profile Management General Settings

Setting	What to Enter
Security type	From Security type drop-down list, choose the method that is used to authenticate a connection to the wireless network. The choices are the following: • No authentication (Open) • Shared • WPA2-Personal • WPA-Personal • WPA2-Enterprise • WPA-Enterprise • 802.1X • CCKM
Encryption type	Encryption choices are determined by the security type that you choose. From the Encryption type drop-down list, choose an available method. The choices are the following: • If you choose No authentication (Open), your encryption choice is None or WEP. • If you choose Shared, your only encryption choice is WEP. • If you choose WPA2-Personal you can choose AES or TKIP. • If you choose WPA-Personal, you can choose AES or TKIP. • If you choose, WPA2-Enterprise, you can choose AES, TKIP, AES (MFP), TKIP (MFP). • If you choose WPA-Enterprise, you can choose AES or TKIP. • If you choose 802.1x, your only encryption choice is WEP. • If you choose CCKM, you can choose AES, WEP, or TKIP.
Network security key	Enter the network security key that you obtain from the network administrator. **Note** The Network security key field only appears when you choose No authentication (Open) with WEP encryption, Shared, WPA2-Personal, or WPA-Personal as the security type.

Table 2-3 Profile Management General Settings (continued)

Setting	What to Enter
Choose a network authentication method	From the Choose a network authentication method drop-down list, choose an authentication method. The choices are the following: • Smart Card or other certificate • Protected EAP (PEAP) • LEAP • PEAP-GTC • EAP-FAST **Note** Smart Card and Protected EAP (PEAP) are provided by Microsoft. These methods were not tested by Cisco on the CB21AG or the PI21AG client adapter. **Note** The Choose a network authentication method drop-down list appears only when you choose WPA2-Enterprise, WPA-Enterprise, 802.1X, or CCKM as the security type. **Note** After you choose the network authentication method, click the **Settings** button to configure the authentication methods. For more information about the authentication method settings, see the EAP-FAST, PEAP-GTC, and LEAP administrator guides.
Cache user information for subsequent connections to this network	Check this check box if you want user information stored for later connections through this profile to the network. **Note** The Cache user information for subsequent connections to this network check box appears only when you choose WPA2-Enterprise, WPA-Enterprise, 802.1X, or CCKM as the security type. These security types rely on a network authentication method that requires user credentials.

Radio Measurement

You can enable or disable the radio measurement feature in the Cisco Connection Settings dialog box, which is available from the profile's Connection tab in the Wireless Network properties dialog box (see Step 2 in the "Viewing and Changing the Settings of a Profile" section on page 2-13 to get to the Cisco Connection Settings dialog box).

When you check the **Enable Radio Measurement** check box, the radio measurement feature is enabled. The client driver advertises support for the Cisco wireless LAN radio measurement feature by including a radio measurement information element when the client associates with the access point. The client can then service radio measurement requests that the network infrastructure sends.

When you uncheck the **Enable Radio Measurement** check box, the client does not advertise the radio measurement information element. The client cannot service radio measurement requests that the network infrastructure sends.

Advanced Roaming Setting

You can enable or disable the advanced roaming feature in the Cisco Connection Settings dialog box, which is available from the profile's Connection tab in the Wireless Network properties dialog box (see Step 2 in the "Viewing and Changing the Settings of a Profile" section on page 2-13 to get to the Cisco Connection Settings dialog box).

Check the **Enable Advanced Roaming Setting** check box to enable the advanced roaming feature. Uncheck the check box to disable the feature.

You can choose from five roaming policies to meet the needs of your wireless network. The roaming policy is the level of aggressiveness for roaming. From the Roaming Option drop-down list, choose roaming policy:

- Very Low—Roaming aggressiveness is very low. The client maintains connection with the current access point until its RSSI and transmit rate drop to the values where it may loose connection. The client roams to another access point only when it might loose connection with the current access point. This roaming policy prioritizes connection to the current AP rather than performance. This policy is best suited for environments in which only one access point is present.
- Low—Roaming aggressiveness is low. The client maintains connection with the current access point until its RSSI and transmit rate drop to values where performance is heavily degraded. This policy is best suited for environments in which access points are distributed sparsely.
- Normal—Roaming aggressiveness is normal. The client maintains connection with the current access point until its RSSI and transmit rate drop to values where performance is degraded. This policy gives balanced priorities to roaming aggressiveness and performance.
- High—Roaming aggressiveness is high. The RSSI and rate thresholds are set to high values to increase the aggressiveness of roaming. This policy is best suited for environments in which many access points are closely distributed and in which the user moves around at a faster pace.
- Very High—Roaming aggressiveness is very high. The RSSI and rate thresholds are set to values that give the best performance. This policy is best suited for environments in which multiple access points are present and in which the user can switch to the best performing access points at any time.
- Default—The default roaming policy is Normal. This roaming policy is set in the client driver.