



## Profile Settings Tab

---

This chapter describes ACAT profile options. The following topics are covered in this section:

- [Adding Profiles, page 4-2](#)
- [Editing Profiles Using the Profile Settings Tab, page 4-4](#)

## Adding Profiles

ACAT enables you to import existing configuration profiles or create new profiles. The ACAT File menu contains two profile options:

- **Create/Manage Profile**—This option enables you to add, delete, or rename new profile names. When profile names are defined, you can use the ACAT Profile Settings tab to configure each of the profiles.
- **Load from Registry**—This option imports or loads existing profiles from your PC's registry into the ACAT configuration file.

The ACU enables you to create and verify profiles prior to distributing them to other users. The profiles created with the ACU are stored in your PC's registry. When you are satisfied that the profiles are correct and operational, you can use the ACAT Load from Registry option to import the profiles for a specific client adapter type into the ACAT configuration file.

Profiles are stored in the part of the registry reserved for the client adapter driver and therefore are tied to a specific radio type. Consequently, if you set up profiles for a 350 series PC card and the client adapter is later upgraded to a CB20A PC card, all of the profiles are not usable for the new client adapter.

## General Recommendations

When you need to configure multiple client adapter types, you should consider the following recommendations:

- On a server accessible to all users, create and name a directory for each client adapter type.
- Place a copy of all the Install Wizard files and sub-directories into each of the client adapter directories.
- Create an ACAT configuration file with the needed profiles and configuration parameters for each client adapter type. Save each ACAT configuration file into the appropriate client adapter directory with the Install Wizard files.



**Note**

---

All ACAT configuration files use the same filename (CiscoAdminConfig.dat) and therefore must be saved separately.

---

- To install profiles for a specific client adapter type, each user must execute the Install Wizard (IWSetup.exe) in the appropriate client adapter directory for their client adapter type.

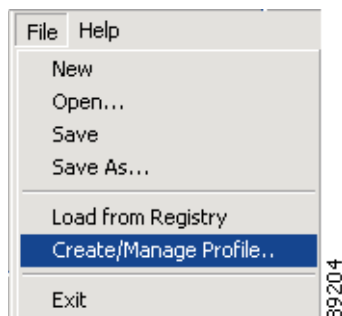
## Create/Manage Profile

Prior to configuring a profile in ACAT, you must create a new profile name for each profile. The Create/Manage Profile option in the File menu enables you to add, delete, or rename new profile names. A maximum of 16 profiles can be created.

To create new profile names, follow these steps:

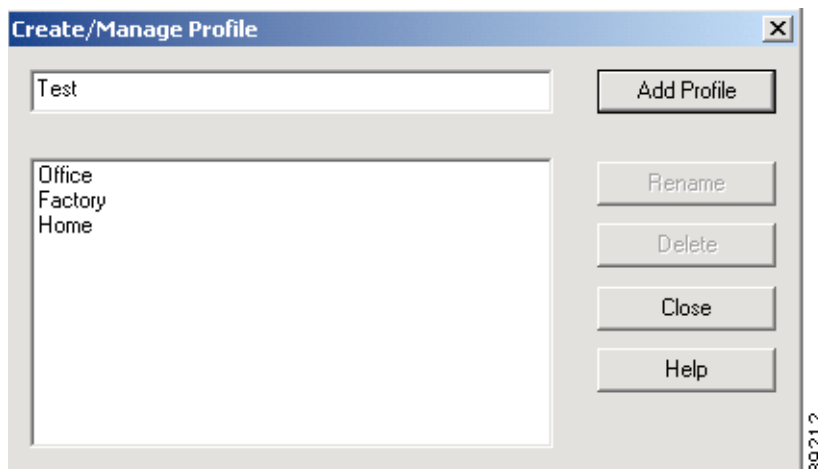
- Step 1** Choose **Create/Manage Profile** in the ACAT File menu (see [Figure 4-1](#)).

**Figure 4-1** Create/Manage Profile Option



When you choose this option, the Create/Manage Profile window appears (see [Figure 4-2](#)).

**Figure 4-2** Create/Manage Profile Window



- Step 2** Enter a new profile name (1 to 79 ASCII characters) in the entry field and click **Add Profile**.
- Step 3** To rename or delete a profile name, click the profile name and click **Rename** or **Delete**.
- Step 4** When you have completed the entry of new profile names, click **Close**.



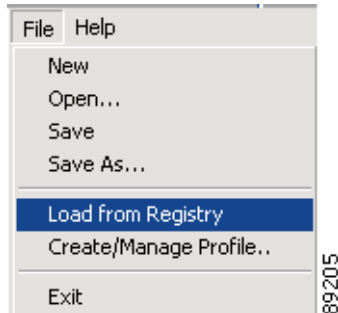
**Note** A maximum of 16 profiles can be created.

To enter profile configuration parameters, go to the [“Editing Profiles Using the Profile Settings Tab”](#) section on page 4-4.

## Load From Registry

The ACAT utility enables you to import existing profiles from your PC's registry by using the Load from Registry option located in the File menu (see [Figure 4-3](#)).

**Figure 4-3** Load from Registry Option



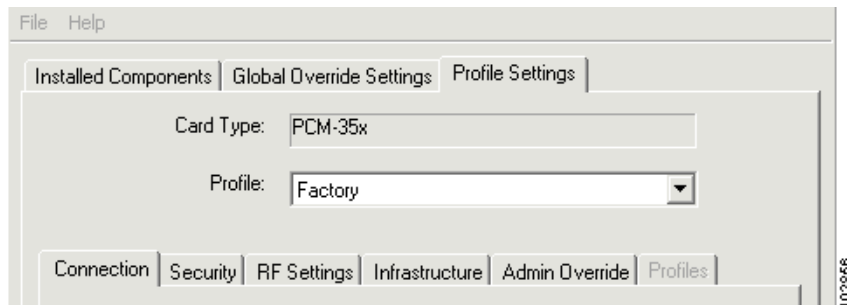
Prior to selecting this option, you must create new profiles using the ACU. These profiles are saved in your PC's registry.

To view or edit the imported profile parameters, go to the “[Editing Profiles Using the Profile Settings Tab](#)” section on page 4-4.

## Editing Profiles Using the Profile Settings Tab

The ACAT Profile Settings tab enables you to edit existing profiles and new profiles being created (see [Figure 4-4](#)).

**Figure 4-4** Profile Settings Tab Window



This section includes the following topics:

- [Card Type, page 4-5](#)
- [Profile, page 4-5](#)
- [Connection Tab, page 4-6](#)
- [Security Tab, page 4-10](#)
- [RF Settings Tab, page 4-26](#)
- [Infrastructure Tab, page 4-32](#)
- [Ad Hoc Tab, page 4-35](#)
- [Admin Override Tab, page 4-37](#)
- [Auto Profile Selection, page 4-38](#)

## Card Type

The Card Type field specifies the client adapter card type being used in the profiles. You specify the card type when you select the New option in the File menu. ACAT defaults to the 350 series PCMCIA (PCM-35x) card type. The following card types are supported:

- PCM-35x—Cisco Aironet 350 series PCMCIA card
- MPI-35x—Cisco Aironet 350 series Mini-PCI card
- PCI-35x—Cisco Aironet 350 series PCI card
- CB20A—Cisco Aironet 5-GHz PC-Cardbus card

**Note**

---

ACAT 1.6 is compatible only with Install Wizard 1.6.

---

**Note**

---

ACAT 1.6 does not support the Cisco Aironet 340 and 4800 series client adapters or the Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG).

---

## Profile

The Profile field enables you to select the profile to be configured. You can click the arrow on the right of the field to view the profile list.

## Connection Tab

The Connection tab enables you to specify connection-specific parameters and the client adapter power save mode. The window is shown in [Figure 4-5](#).

**Figure 4-5** Connection Tab Window

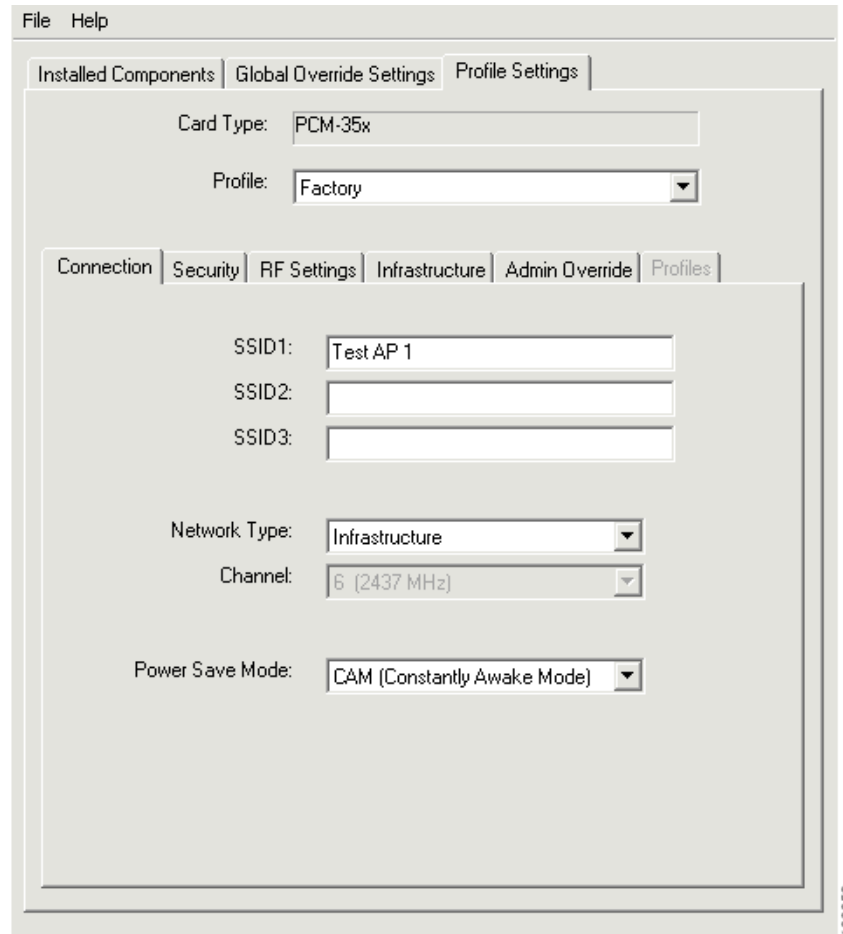


Table 4-1 lists and describes the Connection tab parameters.

**Table 4-1 Connection Tab Parameters**

Parameter	Description						
SSID1	<p>The service set identifier (SSID) identifies the specific wireless network that you want to access.</p> <p><b>Range:</b> You can enter up to 32 ASCII characters (case sensitive)</p> <p><b>Default:</b> A blank field</p> <p><b>Note</b> If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (refer to your access point documentation). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter is unable to access the network.</p>						
SSID2	<p>An optional SSID that identifies a second distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p><b>Note</b> A profile with multiple SSIDs cannot be used in auto profile switching.</p> <p><b>Range:</b> You can enter up to 32 ASCII characters (case sensitive)</p> <p><b>Default:</b> A blank field</p>						
SSID3	<p>An optional SSID that identifies a third distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p><b>Note</b> A profile with multiple SSIDs cannot be used in auto profile switching.</p> <p><b>Range:</b> You can enter up to 32 ASCII characters (case sensitive)</p> <p><b>Default:</b> A blank field</p>						
Network Type	<p>Specifies the type of network in which your client adapter is installed.</p> <p><b>Options:</b> Ad Hoc or Infrastructure</p> <p><b>Default:</b> Infrastructure</p> <table border="1"> <thead> <tr> <th>Network Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Ad Hoc</td> <td>Often referred to as <i>peer to peer</i>. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.</td> </tr> <tr> <td>Infrastructure</td> <td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td> </tr> </tbody> </table>	Network Type	Description	Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.	Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.
Network Type	Description						
Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.						
Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.						

Table 4-1 Connection Tab Parameters (continued)

Parameter	Description
Channel	<p data-bbox="644 317 1485 411">Specifies which frequency your client adapter uses as the channel for communications. These channels conform to the IEEE 802.11 standard for your regulatory domain.</p> <ul data-bbox="656 426 1481 625" style="list-style-type: none"> <li data-bbox="656 426 1481 548">• In infrastructure mode, this parameter is set automatically and cannot be changed. The client adapter listens to the entire spectrum, selects the best access point to associate to, and uses the same frequency as that access point.</li> <li data-bbox="656 569 1481 625">• In ad hoc mode, you must set the channel of the client adapter to match the channel used by the other clients in the wireless network.</li> </ul> <p data-bbox="644 642 1377 674"><b>Range:</b> Dependent on client adapter radio and regulatory domain</p> <p data-bbox="691 686 1110 718">Example for 2.4-GHz client adapters:</p> <p data-bbox="740 732 1260 764">1 to 11 (2412 to 2462 MHz) in North America</p> <p data-bbox="691 779 1089 810">Example for 5-GHz client adapters:</p> <p data-bbox="740 825 1471 882">36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz) in North America</p> <p data-bbox="644 898 1386 930"><b>Default:</b> Dependent on client adapter radio and regulatory domain</p> <p data-bbox="691 945 1110 976">Example for 2.4-GHz client adapters:</p> <p data-bbox="740 991 1102 1022">6 (2437 MHz) in North America</p> <p data-bbox="691 1037 1089 1068">Example for 5-GHz client adapters:</p> <p data-bbox="740 1083 1117 1115">36 (5180 MHz) in North America</p>

Table 4-1 Connection Tab Parameters (continued)

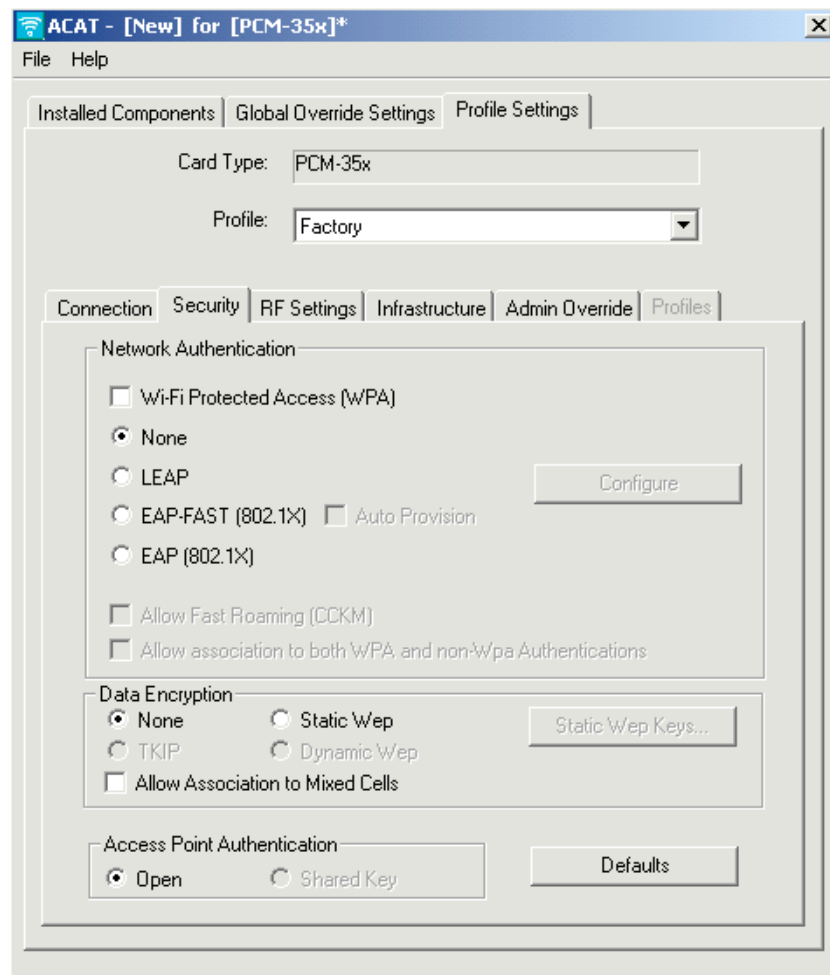
Parameter	Description								
Power Save Mode	<p>Sets your client adapter to its optimum power consumption setting.</p> <p><b>Options:</b> CAM, Max PSP, or Fast PSP</p> <p><b>Default:</b> CAM (Constantly Awake Mode)</p>								
	<table border="1"> <thead> <tr> <th>Power Save Mode</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CAM (Constantly Awake Mode)</td> <td> <p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p> </td> </tr> <tr> <td>Max PSP (Max Power Savings)</td> <td> <p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p> </td> </tr> <tr> <td>Fast PSP (Power Save Mode)</td> <td> <p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p> </td> </tr> </tbody> </table>	Power Save Mode	Description	CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p>	Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p>	Fast PSP (Power Save Mode)	<p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p>
Power Save Mode	Description								
CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p>								
Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p>								
Fast PSP (Power Save Mode)	<p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p>								

## Security Tab

The Security tab window (see [Figure 4-6](#)) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. The Security tab window is organized into three sections:

- Network Authentication—specifies network authentication options.
- Data Encryption—specifies data encryption options.
- Access Point Authentication—specifies access point authentication options.

**Figure 4-6** Security Tab Window



This window presents several security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. [Chapter 5, “Security Features,”](#) provides an overview of the security features.

## Network Authentication

The network authentication section specifies the network authentication options available for your client adapter. [Table 4-2](#) describes the parameter options.

**Table 4-2** Network Authentication Parameters

Parameter	Description
Wi-Fi Protected Access (WPA)	<p>Specifies whether WPA authentication is used by the client adapter.</p> <p><b>Note</b> When WPA is selected, the TKIP data encryption parameter is automatically set. The other data encryption options are unavailable.</p> <p><b>Note</b> When WPA is selected, you can also select LEAP (WPA), EAP-FAST (WPA), or EAP (WPA) authentication.</p> <p><b>Range:</b> selected or not selected</p> <p><b>Default:</b> not selected</p>
None	<p>When selected, specifies that network authentication is not used.</p> <p><b>Range:</b> selected or not selected</p> <p><b>Default:</b> selected</p>
LEAP	<p>Specifies whether LEAP authentication is used by the client adapter.</p> <p><b>Note</b> When LEAP is selected, the Dynamic WEP data encryption option is automatically set. If WPA is selected also, the TKIP data encryption option is automatically set. The other data encryption options are unavailable and the Configure button is activated for entry of LEAP settings.</p> <p><b>Note</b> When WPA is selected this parameter changes from LEAP to LEAP (WPA).</p> <p><b>Range:</b> selected or not selected</p> <p><b>Default:</b> not selected</p>

Table 4-2 Network Authentication Parameters (continued)

Parameter	Description
EAP-FAST (802.1X)	<p>Specifies whether EAP-FAST authentication is used by the client adapter.</p> <p><b>Note</b> When EAP-FAST is selected, the Dynamic WEP data encryption option is automatically set and the Configure button is activated for entry of EAP-FAST settings. If WPA is selected also, the TKIP data encryption option is automatically set. The other data encryption options are unavailable.</p> <p><b>Note</b> This feature is only available when using 350 series or CB20A cards and client adapters.</p> <p><b>Note</b> When WPA is selected this parameter changes from EAP-FAST (802.1X) to EAP-FAST (WPA).</p> <p><b>Note</b> This feature installs only on PCs running the Windows 2000 or XP operating systems. The Install Wizard does not provide an error message when a profile with EAP-FAST fails to install on a non-supported operating system.</p> <p><b>Range:</b> selected or not selected  <b>Default:</b> not selected</p>
Auto Provision	<p>Specifies whether EAP-FAST authentication uses automatically accessed or manually specified Protected Authentication Credentials (PAC) provisioning.</p> <p><b>Note</b> Provisioning is the process of associating a PAC file with a specific user or group of users.</p> <p><b>Note</b> When auto provisioning is not selected, the ACU must be used to enter the provisioning information.</p> <p><b>Range:</b> selected or not selected  <b>Default:</b> not selected</p>
EAP (802.1X)	<p>Specifies whether the client adapter uses an 802.1X authentication type supported by your PC operating system.</p> <p><b>Note</b> When WPA is selected this parameter changes from EAP (802.1X) to EAP (WPA).</p> <p><b>Range:</b> selected or not selected  <b>Default:</b> not selected</p>

**Table 4-2** Network Authentication Parameters (continued)

Parameter	Description
Allow Fast Roaming (CCKM)	<p>Specifies whether the client adapter can use the CCKM feature available in some access points.</p> <p><b>Note</b> This option is available only when LEAP or EAP-FAST is selected.</p> <p><b>Note</b> When this option is selected, the client adapter uses CCKM only with access points supporting the CCKM feature but the client adapter can associate with access points that do not support CCKM.</p> <p><b>Range:</b> selected or not selected</p> <p><b>Default:</b> not selected</p>
Allow association to both WPA and non-WPA Authentications	<p>Specifies whether the client adapter can associate to access points supporting or not supporting WPA.</p> <p><b>Note</b> This option is only available when WPA is selected.</p> <p><b>Range:</b> selected or not selected</p> <p><b>Default:</b> not selected</p>

## Data Encryption

The Data Encryption section specifies the encryption options (see [Table 4-3](#)) used by the client adapter.

**Table 4-3** Data Encryption Options

Parameter	Description
None	<p>Specifies that data encryption is not used by the client adapter.</p> <p><b>Range:</b> selected or unselected</p> <p><b>Default:</b> selected</p>
Static WEP	<p>Specifies that static WEP encryption is used by the client adapter.</p> <p><b>Range:</b> selected or unselected</p> <p><b>Default:</b> unselected</p>
TKIP	<p>Specifies that Temporal Key Integrity Protocol (TKIP) is used by the client adapter.</p> <p><b>Note</b> TKIP is automatically enabled when WPA is selected.</p> <p><b>Range:</b> selected or unselected</p> <p><b>Default:</b> unselected</p>

Table 4-3 Data Encryption Options (continued)

Parameter	Description
Dynamic WEP	<p>Specifies that dynamic WEP encryption is used by the client adapter.</p> <p><b>Note</b> Dynamic WEP is automatically enabled when LEAP or EAP-FAST is selected.</p> <p><b>Range:</b> selected or unselected</p> <p><b>Default:</b> unselected</p>
Allow Association to Mixed Cells	<p>Indicates whether the client adapter can associate to an access point that enables both WEP and non-WEP associations.</p> <p><b>Range:</b> selected or unselected</p> <p><b>Default:</b> unselected</p>

## Allow Association To Mixed Cells Parameter

The Allow Association To Mixed Cells parameter indicates whether the client adapter can associate to an access point that enables both WEP and non-WEP associations. Follow the guidelines below to set this parameter.

- Check the **Allow Association To Mixed Cells** check box if the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association To Mixed Cells** check box if the access point with which the client adapter is to associate does not have WEP set to Optional.



**Note** For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP.



**Note** This parameter is not available in Ad Hoc mode.



**Note** This parameter is not available if WPA is selected unless the *Allow association to both WPA and non-WPA Authentications* parameter is also selected.

## Access Point Authentication

The access point authentication section defines how your client adapter attempts to authenticate to an access point:

- **Open Authentication**—Enables your client adapter, regardless of its WEP settings, to associate and attempt to communicate with an access point. Open Authentication is the default setting.



**Note** The client adapter can successfully send data frames only when it has the same WEP key as the access point.

- **Shared Key Authentication**—Enables your client adapter to communicate only with access points that have the same WEP key.

In shared key authentication, the access point sends a known unencrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated.



**Note** Cisco does not recommend the use of shared key authentication because it is a security risk.



**Note** Shared key authentication is only available when Static WEP is selected as the data encryption method.

## Entering a New Static WEP Key

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

**Step 1** Check **None** under the Network Associations section on the Security Tab Window.

**Step 2** Check **Static WEP** under Data Encryption.



**Note** Selecting **LEAP** from the Network Authentication section on the Security tab window automatically disables static WEP and enables dynamic WEP.

**Step 3** Click **Static WEP Keys** and the WEP Key Setting window appears.

**Step 4** Choose one of the following WEP key entry methods using the drop-down menu:

- **Hexadecimal**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.



**Note** ASCII text WEP keys are not supported on Cisco Aironet 1200 Series Access Points (running VxWorks software), so you must select the Hexadecimal (0-9, A-F, a-f) option if you are planning to use your client adapter with these access points.

**Step 5** For the static WEP key that you are entering (1, 2, 3, or 4), select a WEP key size of 40 or 128 using the drop-down menu. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys.

- Step 6** Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:
- WEP keys 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:** 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)
  - Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
  - When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.
- Step 7** Click the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.
- Step 8** Choose one of the following access point authentication options, which defines how your client adapter attempts to authenticate to an access point:
- **Open**—Enables your client adapter to authenticate and attempt to communicate with an access point, regardless of its WEP settings. Open Authentication is the default setting.
  - **Shared Key**—Enables your client adapter to communicate only with access points that have the same WEP key. This option is only available if Static WEP is selected.




---

**Note** Cisco recommends that shared key authentication not be used because it is a security risk.

---

- Step 9** Click **OK** to return to the Security tab window.




---

**Note** After a WEP key is configured, you can enter a new key value, but you cannot view the original key or delete it.

---

## Disabling Static WEP

To disable static WEP for a particular profile, check **None** under Data Encryption on the Security Tab Window.




---

**Note** Selecting **LEAP** from the Network Authentication section on the Security tab window automatically disables static WEP and enables dynamic WEP.

---

## Enabling LEAP

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

- Client adapters must support WEP and use the firmware, drivers, utilities, and security modules included in the Install Wizard file.
- To use WPA, 350 series and CB20A client adapters must use the software included in Install Wizard 1.2 or later on a computer running Windows 2000 or XP operating systems.
- To use the reporting access points that fail LEAP authentication and fast secure roaming features, client adapters must use the client adapter firmware included in Install Wizard 1.2 or later.
- Access points to which your client adapter may attempt to authenticate must use the following software releases or later: VxWorks release 11.23T (340 and 350 series access points), 11.54T (1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).



---

**Note** To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use the reporting access points that fail LEAP authentication and fast secure roaming features, access points must use the VxWorks release 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).

---

- All necessary infrastructure devices (such as access points, servers, etc.) must be properly configured for LEAP authentication.

Follow these steps to enable LEAP authentication for the selected profile.

---

**Step 1** If you want to enable WPA, check **Wi-Fi Protected Access (WPA)** on the Network Authentication section of the Security tab window. This parameter enables client adapters to associate to access points using WPA (for additional information refer to [“Wi-Fi Protected Access \(WPA\)” section on page 5-6](#)).

**Step 2** Check **LEAP** on the Network Authentication section of the Security tab window.



---

**Note** When you check this option, dynamic WEP is automatically enabled. If WPA is also selected, TKIP is enabled.

---

**Step 3** Click **Configure** and the LEAP Settings window appears (see [Figure 4-7](#)).

**Figure 4-7** LEAP Settings Window

**Step 4** Choose one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password**—Requires the entry of a LEAP username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password**—Uses the LEAP username and password saved by the ACU in the computer’s registry each time the computer reboots. Authentication occurs automatically as needed using the saved username and password (which are registered with the RADIUS server).



**Note** When this option is selected, you must use the ACU on their PCs to configure LEAP by selecting the *Use Saved User Name and Password* option and entering the appropriate LEAP username and password. The option fields are unavailable in ACAT.



**Note** The Use Saved User Name and Password option is available only if the Allow Saved LEAP User Name and Password option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window”](#) section on page 2-2 for additional information).

- Step 5** If you selected Use Temporary User Name and Password in [Step 4](#), choose one of the following options using the drop-down menu:
- **Use Windows User Name and Password**—Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for LEAP User Name and Password**—Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for LEAP User Name and Password**—Requires you to manually invoke the LEAP authentication process as needed using the Manual LEAP Login option from the ACU Commands drop-down menu. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- Step 6** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is not selected.
- Step 7** If you work in an environment with multiple domains and want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Login Domain With User Name** check box. The default setting is not selected.
- Step 8** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is checked.
- Step 9** In the LEAP Authentication Timeout Value field, enter the amount of time (in seconds) after which a LEAP authentication is considered a failure and an error message appears.
- Range:** 45 to 300 seconds
- Default:** 90 seconds
- Step 10** If you want to limit the amount of time that is spent finding a domain controller during the authentication process, follow these steps:
- a. Check **Restrict Time Finding the Domain Controller to (seconds)**.  
**Default:** Unchecked
  - b. Enter the amount of time (in seconds) allowed in the authentication process to find the domain controller. Finding the domain controller is the last sequence of the authentication process.  
**Range:** 0 to 300 seconds  
**Default:** 0 seconds

**Note**

---

Entering a value of zero causes the authentication process to skip the “Finding Domain Controller” step altogether.

---

**Note**

---

The finding domain controller timeout value is included in the overall LEAP authentication timeout value. For example, if the authentication timeout value is 60 seconds, and the finding domain controller timeout value is 10 seconds, the client adapter has up to 60 seconds to complete the entire authentication process, up to 10 seconds of which is allocated for finding the domain controller.

---




---

**Note** If you require domain services such as login scripts and roaming desktops, Cisco recommends that you do not check the Restrict Time Finding Domain Controller to (seconds) check box.

---




---

**Note** Regardless of whether the check box is checked or unchecked, the “Finding Domain Controller” step is bypassed once you are logged into Windows or if you log into the local machine and not into a domain.

---

**Step 11** Click **OK** to exit the LEAP Settings window and return to the Security tab window.

**Step 12** If you want to enable fast roaming on your client adapter, check **Allow Fast Roaming (CCKM)** in the Network Authentication section of the Security tab window.

- Selecting this option enables the client adapter to use CCKM when associated to access points that are using CCKM. Using this option your client adapter can also associate to access points that are not using CCKM.
- Not selecting this option prevents your client adapter from using CCKM even with access points that use CCKM.

**Default:** Not selected




---

**Note** This option is available only when WPA is enabled.

---




---

**Note** If your computer uses the Microsoft 802.1X supplicant and you want to take advantage of the fast roaming feature, refer to the Microsoft documentation for instructions.

---

**Step 13** If you want to associate to access points that support WPA and even those that do not support it, check **Allow Association to both WPA and non-WPA authentication**. If this option is not selected, your client adapter can associate only to access points that use WPA.

**Default:** Not selected

---

## Enabling EAP-FAST

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

- Client adapters must support WEP and use the firmware, drivers, utilities, and security modules included in the Install Wizard file.
- The 350 series and CB20A client adapters must use the software included in Install Wizard 1.3 or later on a computer running Windows 2000 or XP operating systems.
- To use the reporting access points that fail EAP-FAST authentication and fast secure roaming features, client adapters must use the client adapter firmware included in Install Wizard 1.3 or later.
- Access points to which your client adapter may attempt to authenticate must use the following software releases or later: VxWorks release 11.23T (340 and 350 series access points), 11.54T (1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).



---

**Note** To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use the reporting access points that fail EAP-FAST authentication and fast secure roaming features, access points must use the VxWorks release 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).

---

- All necessary infrastructure devices (such as access points, servers, etc.) must be properly configured for EAP-FAST authentication.

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

---

**Step 1** If you want to enable WPA, check **Wi-Fi Protected Access (WPA)** on the Network Authentication section of the Security tab window. This parameter enables client adapters to associate to access points using WPA (for additional information refer to [“Wi-Fi Protected Access \(WPA\)” section on page 5-6](#)).

**Step 2** Check **EAP-FAST** on the Network Authentication section of the Security tab window.



---

**Note** When you check this option, dynamic WEP is automatically enabled. If WPA is also selected, TKIP is enabled.

---

**Step 3** Check **Auto Provision** to allow the EAP-FAST protocol to transmit the username and password to the EAP-FAST server to automatically obtain the PAC provisioning.



---

**Note** The Auto Provision option is available only if the Allow Auto Provisioning option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window” section on page 2-2](#) for additional information).

---



---

**Note** If Auto-Provision is not checked, the ACU must be used to manually configure the PAC settings for this profile.

---

**Step 4** Click **Configure** and the EAP-FAST Settings window appears (see [Figure 4-8](#)).

**Figure 4-8** EAP-FAST Settings Window

**Step 5** Check one of the following EAP-FAST username and password setting options:

- **Use Temporary User Name and Password**—Requires the entry of an EAP-FAST username and password each time the computer reboots in order to authenticate and gain access to the network. This option is the default setting.
- **Use Saved User Name and Password**—Uses the EAP-FAST username and password saved by the ACU in the computer’s registry each time the computer reboots. Authentication occurs automatically as needed using the saved username and password (which are registered with the EAP-FAST server).



**Note**

When this option is selected, you must use the ACU to configure EAP-FAST by selecting the *Use Saved User Name and Password* option and entering the appropriate EAP-FAST username and password. The option fields are unavailable in ACAT.



**Note**

The Use Saved User Name and Password option is available only if the Allow Saved EAP-FAST User Name and Password option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window”](#) section on page 2-2 for additional information).

- Step 6** If you selected Use Temporary User Name and Password in [Step 4](#), choose one of the following options using the drop-down menu:
- **Use Windows User Name and Password**—Causes your Windows username and password to also serve as your EAP-FAST username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires you to enter a separate EAP-FAST username and password (which are registered with the EAP-FAST server) in addition to your regular Windows login in order to start the EAP-FAST authentication process.
  - **Manually Prompt for User Name and Password**—Requires you to manually invoke the EAP-FAST authentication process as needed using the Manual EAP-FAST Login option from the ACU Commands drop-down menu. You are not prompted to enter a EAP-FAST username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- Step 7** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is not selected.
- Step 8** If you work in an environment with multiple domains and want your Windows login domain to be passed to the EAP-FAST server along with your username, check the **Include Windows Login Domain With User Name** check box. The default setting is not selected.
- Step 9** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is checked.
- Step 10** In the Authentication Timeout Value field, enter the amount of time (in seconds) before a EAP-FAST authentication is considered a failure and an error message appears.
- Range:** 45 to 300 seconds
- Default:** 90 seconds
- Step 11** If you want to limit the amount of time that is spent finding a domain controller during the authentication process, follow these steps:
- a. Check **Restrict Time Finding the Domain Controller to (seconds)**.
- Default:** Unchecked
- b. Enter the amount of time (in seconds) allowed in the authentication process to find the domain controller. Finding the domain controller is the last sequence of the authentication process.
- Range:** 0 to 300 seconds
- Default:** 0 seconds

**Note**

---

Entering a value of zero causes the authentication process to skip the “Finding Domain Controller” step altogether.

---

**Note**

---

The finding domain controller timeout value is included in the overall EAP-FAST authentication timeout value. For example, if the authentication timeout value is 60 seconds, and the finding domain controller timeout value is 10 seconds, the client adapter has up to 60 seconds to complete the entire authentication process, up to 10 seconds of which is allocated for finding the domain controller.

---




---

**Note** If you require domain services such as login scripts and roaming desktops, Cisco recommends that you do not check the Restrict Time Finding Domain Controller to (seconds) check box.

---




---

**Note** Regardless of whether the check box is checked or unchecked, the “Finding Domain Controller” step is bypassed once you are logged into Windows or if you log into the local machine and not into a domain.

---

**Step 12** Click **OK** to exit the EAP-FAST Settings window and return to the Security tab window.

**Step 13** If you want to enable fast roaming on your client adapter, check **Allow Fast Roaming (CCKM)** in the Network Authentication section of the Security tab window.

- Selecting this option enables the client adapter to use CCKM when associated to access points that are using CCKM. Using this option your client adapter can also associate to access points that are not using CCKM.
- Not selecting this option prevents your client adapter from using CCKM even with access points that use CCKM.

**Default:** Not selected




---

**Note** This option is available only when WPA is enabled.

---




---

**Note** If your computer uses the Microsoft 802.1X supplicant and you want to take advantage of the fast roaming feature, refer to the Microsoft documentation for instructions.

---

**Step 14** If you want to associate to access points that support WPA and even those that do not support it, check **Allow Association to both WPA and non-WPA authentication**. If this option is not selected, your client adapter can associate only to access points that use WPA.

**Default:** Not selected

---

## Enabling Host-Based EAP

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

- EAP authentication is supported only by 340 and 350 series access points running VxWorks release 11.06 (or later) or 1200 series access points running VxWorks release 11.40T (or later) or 1100 series access points.
- MIC, TKIP, PEAP, Broadcast Key Rotation, and EAP-SIM authentications are supported only by 340 and 350 series access points running VxWorks release 11.23T (or later), 1200 series access points running VxWorks release 11.54T (or later), or 1100 series access points.
- The Microsoft 802.1X supplicant must be installed on your user’s PCs running Windows.

- To use WPA or WPA-PSK, you must use a 350 series or CB20A client adapter with the software included in Install Wizard 1.2 or later on a computer running Windows 2000 or XP. Also one of the following host supplicants must be installed. You can download these supplicants from the URLs provided:
  - Funk Odyssey Client supplicant release 2.2 (for Windows 2000)  
[http://www.funk.com/radius/wlan/wlan\\_c\\_radius.asp](http://www.funk.com/radius/wlan/wlan_c_radius.asp)
  - Windows XP Service Pack 1 and Microsoft supplicant Q815485 (for Windows XP)  
<http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp>  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en>




---

**Note** To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later.

---




---

**Note** For additional information on configuring WPA or WPA-PSK on Microsoft Window PCs, refer to Microsoft documentation and the Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows..

---

- All necessary infrastructure devices (for example, access points, servers, gateways, user databases, etc.) must be properly configured for the authentication type you plan to enable on the client.

Follow the steps below to enable host-based EAP authentication (EAP-TLS, PEAP, or EAP-SIM) for this profile.




---

**Note** Because EAP-TLS, PEAP, and EAP-SIM authentication are enabled in the operating system and not in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. You can create a profile that uses host-based EAP, but you must enable the specific authentication type in Windows (provided Windows uses the Microsoft 802.1X supplicant). In addition, Windows can be set for only one authentication type at a time; therefore, if you have more than one profile that uses host-based EAP and you want to use another authentication type, you must change authentication types in Windows after switching profiles in ACU.

---

- 
- Step 1** Check **Wi-Fi Protected Access (WPA)** under Network Authentication on the Security tab window if you want to enable WPA. This parameter enables the client adapter to associate to access points using WPA.
- Step 2** Check **Host Based EAP** from the Network Authentication on the Security tab window.
- Step 3** Dynamic WEP Keys are used if your access point is configured for EAP-TLS, PEAP, and EAP-SIM authentication. Click **Dynamic WEP** if WPA is not enabled.




---

**Note** For additional information on configuring a PC running Windows 2000 or XP, refer to Microsoft documentation or the *Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*.

---

## RF Settings Tab

The RF Settings tab window (see [Figure 4-9](#)) enables you to set parameters that control how and when the client adapter transmits and receives data.

**Figure 4-9** RF Settings Tab Window

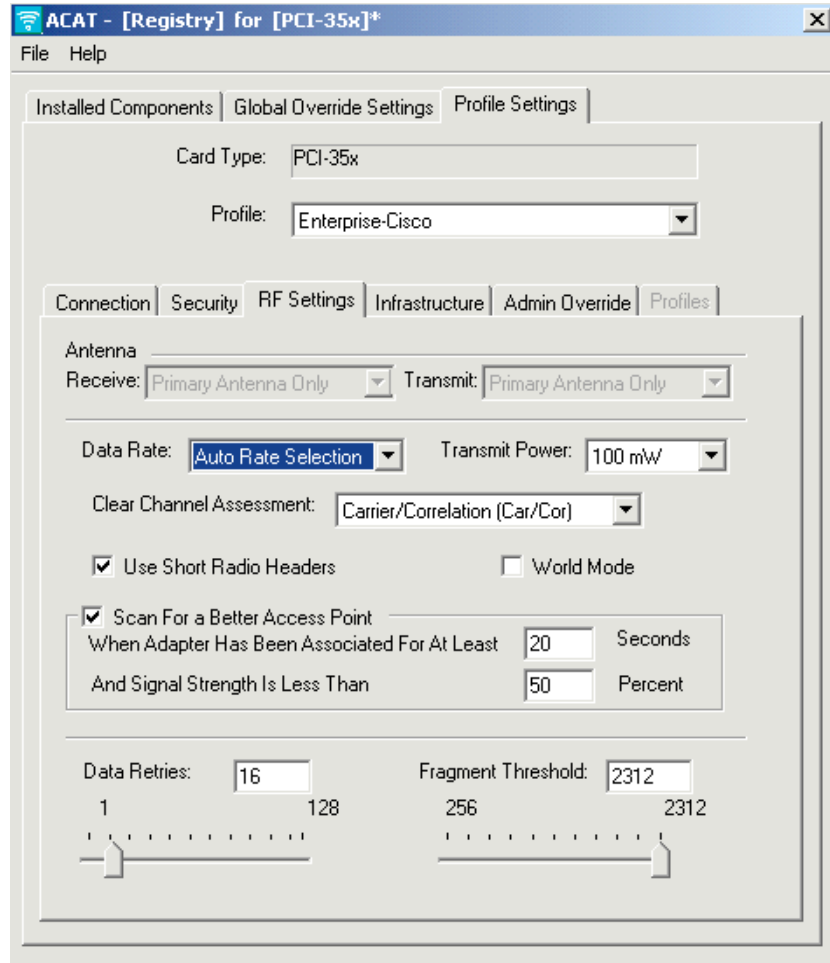


Table 4-4 lists and describes the client adapter's RF network parameters. Follow the instructions in the table to change any parameters.

**Table 4-4** RF Network Parameters

Parameter	Description
Antenna (Receive)	<p>Specifies the antenna that your client adapter uses to receive data.</p> <ul style="list-style-type: none"> <li>PCM and CB20A cards—The integrated, permanently attached antennas operates best when used in diversity mode. Diversity mode enables the card to use the better signal from its two antenna ports. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> <li>PCI card—The PCI card must use the Primary Antenna Only option. <b>Default:</b> Primary Antenna Only</li> <li>MPI card—The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode enables the card to use the better signal from its two antenna connectors. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> </ul> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p>
Antenna (Transmit)	<p>Specifies the antenna that your client adapter uses to transmit data. See the Antenna (Receive) parameter above for information on the options available for your client adapter.</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p>

Table 4-4 RF Network Parameters (continued)

Parameter	Description		
Data Rate	<p>Specifies the rate at which your client adapter should transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).</p> <p>Auto Rate Selection is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.</p> <p><b>Options:</b> Auto Rate Selection, 1 Mbps Only, 2 Mbps Only, 5.5 Mbps Only, or 11 Mbps Only (2.4-GHz client adapters)</p> <p>Auto Rate Selection, 6 Mbps Only, 9 Mbps Only, 12 Mbps Only, 18 Mbps Only, 24 Mbps Only, 36 Mbps Only, 48 Mbps Only, or 54 Mbps Only (5-GHz client adapters)</p> <p><b>Default:</b> Auto Rate Selection</p>		
	Data Rate		Description
	2.4-GHz Client Adapters	5-GHz Client Adapters	
	Auto Rate Selection	Auto Rate Selection	Uses the 11-Mbps (for 2.4-GHz client adapters) or 54-Mbps (for 5-GHz client adapters) data rate when possible but drops to lower rates when necessary.
	1 Mbps Only	6 Mbps Only	Offers the greatest range but the lowest throughput.
	2 Mbps Only and 5.5 Mbps Only	9 Mbps Only to 48 Mbps Only	Progressively offers less range but greater throughput than the 1 Mbps Only (for 2.4-GHz client adapters) or 6 Mbps Only (for 5-GHz client adapters) option.
	11 Mbps Only	54 Mbps Only	Offers the greatest throughput but the lowest range.
	<p><b>Note</b> Your client adapter's data rate must be set to Auto Rate Selection or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.</p>		

Table 4-4 RF Network Parameters (continued)

Parameter	Description
Transmit Power	Defines the power level at which your client adapter transmits. This value must not be higher than that allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, MKK in Japan, etc.). <b>Options:</b> Dependent on the power table programmed into the client adapter; see the table below <b>Default:</b> The maximum level programmed into the client adapter and allowed by your country's regulatory agency
	<b>Possible Power Levels</b>
	<b>Client Adapter Type</b>
	100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW
	20 mW, 10 mW, or 5 mW
	PC-Cardbus card (5-GHz client adapter)
<b>Note</b>	Reducing the transmit power level conserves battery power but decreases radio range.
<b>Note</b>	When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.
<b>Note</b>	If you are using an older version of a 350 series client adapter, your power level options may be different than those listed here.

Table 4-4 RF Network Parameters (continued)

Parameter	Description										
Clear Channel Assessment	Specifies the method that determines whether the channel on which your client adapter operates is clear prior to the transmission of data. <b>Options:</b> Firmware Default ( <i>xxx</i> ), Carrier/Correlation (Car/Cor), Energy Detect (ED), or ED or Car/Cor <b>Default:</b> Firmware Default ( <i>xxx</i> )										
	<table border="1"> <thead> <tr> <th>Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Firmware Default (<i>xxx</i>)</td> <td>The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. <b>Note</b> The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</td> </tr> <tr> <td>Carrier/Correlation (Car/Cor)</td> <td>The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</td> </tr> <tr> <td>Energy Detect (ED)</td> <td>The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.</td> </tr> <tr> <td>ED or Car/Cor</td> <td>The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</td> </tr> </tbody> </table>	Method	Description	Firmware Default ( <i>xxx</i> )	The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. <b>Note</b> The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.	Carrier/Correlation (Car/Cor)	The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.	Energy Detect (ED)	The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.	ED or Car/Cor	The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.
	Method	Description									
	Firmware Default ( <i>xxx</i> )	The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. <b>Note</b> The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.									
	Carrier/Correlation (Car/Cor)	The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.									
	Energy Detect (ED)	The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.									
ED or Car/Cor	The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.										
<b>Note</b> This parameter is available only for 2.4-GHz client adapters.											
Use Short Radio Headers	Checking this check box sets your client adapter to use short radio headers. However, the adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then <i>all</i> clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled.  Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers. <b>Default:</b> Selected <b>Note</b> This parameter is available only for 2.4-GHz client adapters in Infrastructure mode. <b>Note</b> This parameter is referred to as <i>Preambles</i> on the access point windows.										

Table 4-4 RF Network Parameters (continued)

Parameter	Description
World Mode	<p>Checking this check box enables the client adapter to adopt the maximum transmit power level and the frequency range of the access point to which it is associated, provided the access point is also configured for world mode. This parameter is available only in infrastructure mode and is designed for users who travel between countries and want their client adapters to associate to access points in different regulatory domains.</p> <p><b>Default:</b> Deselected</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p> <p><b>Note</b> When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.</p>
Periodically Scan For a Better Access Point	<p>Checking this check box causes the client adapter to look for a better access point if the signal strength of its associated access point is less than the specified value after the specified time and to switch associations if it finds one.</p> <p><b>Example:</b> If the default values of 20 seconds and 50% are used, the client adapter begins monitoring the strength of the signal received from its associated access point 20 seconds after becoming associated. The monitoring continues once per second. If the client detects a signal strength reading below 50%, it scans for a better access point.</p> <p><b>Range:</b> 5 to 255 seconds; 0 to 75% signal strength</p> <p><b>Defaults:</b> Checked, 20 seconds, 50% signal strength</p>
Data Retries	<p>Defines the number of times a packet is resent if the initial transmission is unsuccessful.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> If your network protocol performs its own retries, set this parameter to a smaller value than the default. This way, notification of a bad packet is sent up the protocol stack quickly so the application can retransmit the packet if necessary.</p>
Fragment Threshold	<p>Defines the threshold above which an RF data packet is split up or fragmented. If one of those fragmented packets experiences interference during transmission, only that specific packet would need to be resent.</p> <p>Throughput is generally lower for fragmented packets because the fixed packet overhead consumes a higher portion of the RF bandwidth.</p> <p><b>Range:</b> 256 to 2312</p> <p><b>Default:</b> 2312</p>

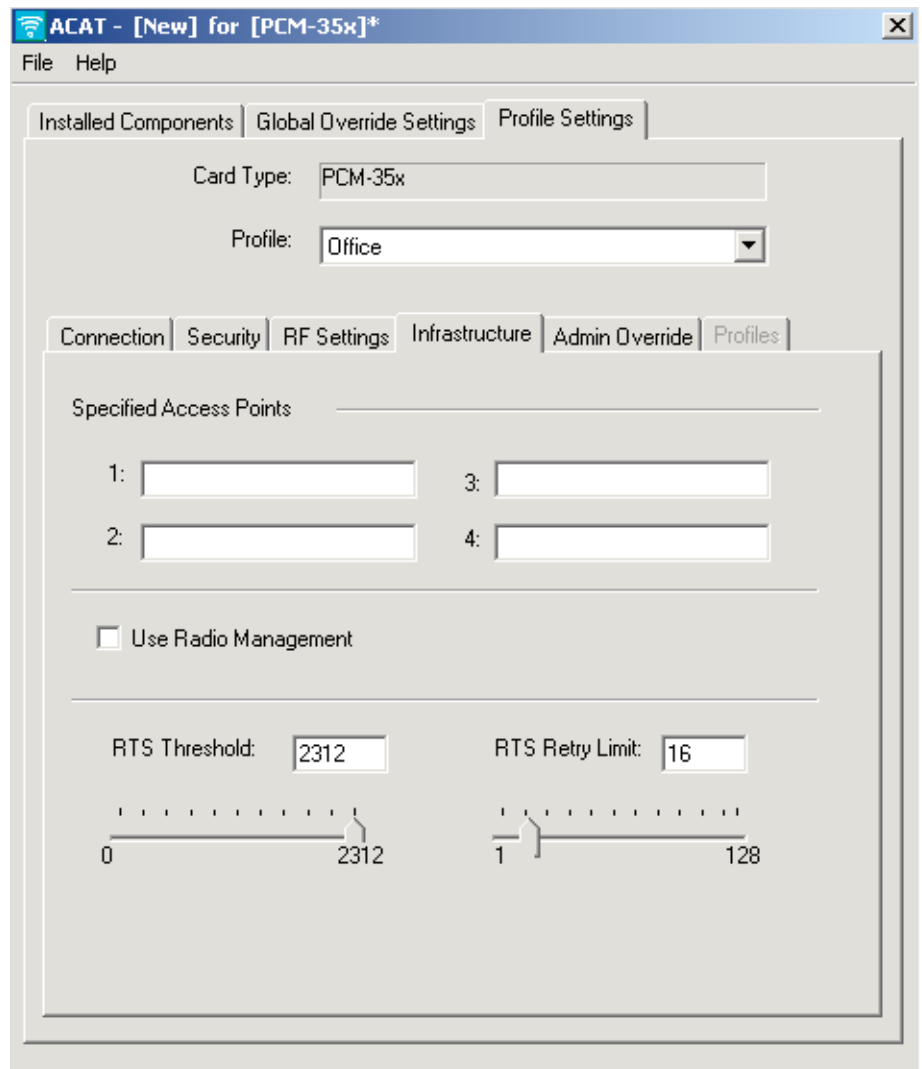
## Infrastructure Tab

The Infrastructure tab window (see [Figure 4-10](#)) enables you to set parameters that control how the client adapter operates within an infrastructure network.


**Note**

You can set infrastructure parameters only if your client adapter is set to operate in an infrastructure network. See the Network Type parameter in [Table 4-1](#).

**Figure 4-10** Infrastructure Tab Window



[Table 4-5](#) lists and describes the client adapter's infrastructure parameters. Follow the instructions in the table to change any parameters.

**Table 4-5 Infrastructure Tab Parameters**

Parameter	Description
Specified Access Points 1-4	<p>Specifies the MAC addresses of up to four preferred access points with which the client adapter can associate. If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.</p> <p>You can enter the MAC addresses of the access points in the edit boxes or choose not to specify access points by leaving the boxes blank.</p> <p><b>Default:</b> Blank fields</p> <p><b>Note</b> This parameter should be used only for access points that are in repeater mode. For normal operation, leave these fields blank because specifying an access point slows down the roaming process.</p>
Use Radio Management	<p>Selecting this parameter enables the access point to which the client adapter is associated to control the use of radio management (RM), provided RM is enabled on the access point. RM is a system-wide feature that involves multiple infrastructure nodes. The RM feature on the access point acts on radio measurement requests from other network devices to instruct the access point and/or its associated clients to perform required radio measurements and then report them.</p> <p><b>Note</b> This parameter is available in Install Wizard version 1.2 or later and only for 350 series client adapters.</p> <p><b>Note</b> Access points must use Cisco IOS Release 12.2(13)JA or later to enable RM. Refer to the documentation for your access point for instructions on enabling this feature.</p> <p><b>Range:</b> Enable or disabled</p> <p><b>Default:</b> Disabled</p>

Table 4-5 Infrastructure Tab Parameters (continued)

Parameter	Description
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced. However, the system is able to recover faster from interference or collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 0 to 2312</p> <p><b>Default:</b> 2312</p> <p><b>Note</b> Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered. However, a large value makes the system more immune to interference and collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>

## Ad Hoc Tab

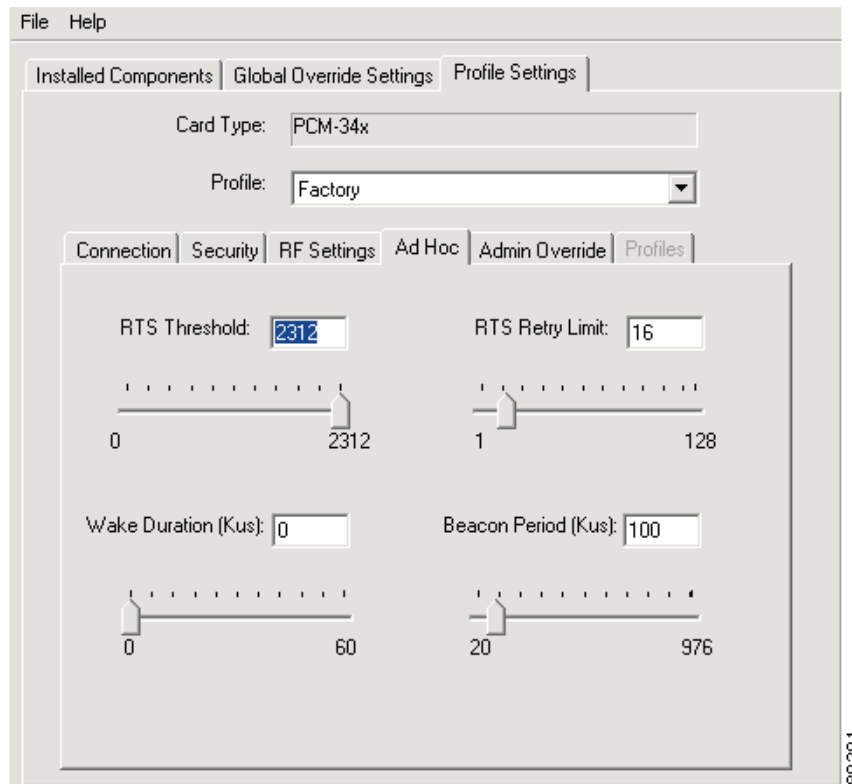
The Ad Hoc tab window (see [Figure 4-11](#)) enables you to set parameters that control how the client adapter operates within an ad hoc network.



**Note**

You can set ad hoc parameters only if your client adapter is set to operate in an ad hoc network. See the network type parameter in [Table 4-1](#).

**Figure 4-11 Ad Hoc Tab Window**



[Table 4-6](#) lists and describes the client adapter's advanced ad hoc parameters. Follow the instructions in the table to change any parameter.

Table 4-6 Ad Hoc Tab Parameters

Parameter	Description
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced. However, the system is able to recover faster from interference or collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 0 to 2312</p> <p><b>Default:</b> 2312</p> <p><b>Note</b> Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered. However, a large value makes the system more immune to interference and collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
Wake Duration (K $\mu$ s)	<p>Specifies the amount of time following a beacon that the client adapter stays awake to receive announcement traffic indication message (ATIM) packets, which are sent to the adapter to keep it awake until the next beacon.</p> <p>Refer to the power save mode parameter in <a href="#">Table 4-1</a>.</p> <p><b>Range:</b> 0 K<math>\mu</math>s (in CAM mode); 5 to 60 K<math>\mu</math>s (in Max PSP or Fast PSP mode)</p> <p><b>Default:</b> 0 K<math>\mu</math>s</p> <p><b>Note</b> If your client adapter is set to CAM mode, you must set the wake duration to 0 K<math>\mu</math>s. If your client adapter is set to Max PSP or Fast PSP mode, you must set the wake duration to a minimum of 5 K<math>\mu</math>s.</p> <p><b>Note</b> K<math>\mu</math>s is a unit of measurement in software terms. K = 1024, <math>\mu</math> = 10<sup>-6</sup>, and s = seconds, so K<math>\mu</math>s = .001024 seconds, 1.024 milliseconds, or 1024 microseconds.</p>

**Table 4-6 Ad Hoc Tab Parameters (continued)**

Parameter	Description
Beacon Period (K $\mu$ s)	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode.  <b>Range:</b> 20 to 976 K $\mu$ s <b>Default:</b> 100 K $\mu$ s

## Admin Override Tab

The Admin Override tab window (see [Figure 4-12](#)) enables you to specify administrator override settings for individual profiles. Each profile can have different settings.


**Note**

The settings on the Global Override Settings tab apply to all profiles and override these individual profile settings.

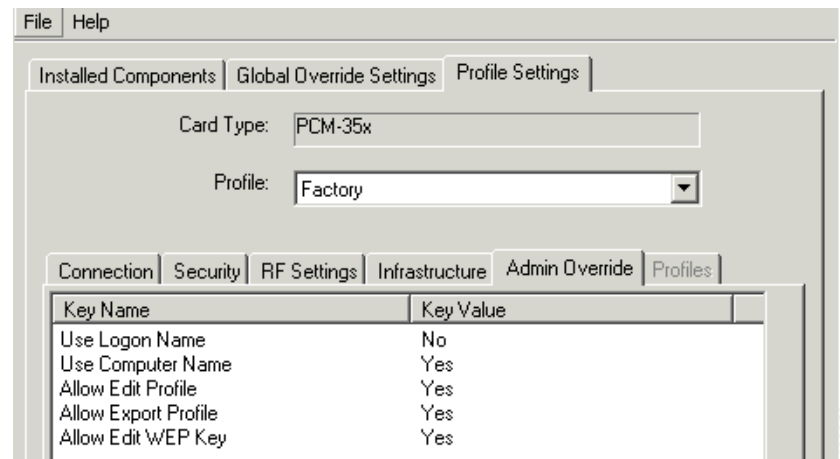
**Figure 4-12 Admin Override Tab Window**

Table 4-7 lists and describes the Admin Override tab parameters. Follow the instructions in the table to change any parameter.

**Table 4-7 Admin Override Tab Parameters**

Parameter	Description
Use Logon Name	Specifies whether the Window's logon name is used as the client's logon name. <b>Range:</b> yes or no <b>Default:</b> no <b>Note</b> When you select <i>Use Logon Name</i> , the Use Computer Name parameter is automatically deselected.
Use Computer Name	Specifies whether your computer's name is used as the client's logon name. <b>Range:</b> yes or no <b>Default:</b> no <b>Note</b> When you select <i>Use Computer Name</i> , the Use Logon Name parameter is automatically deselected.
Allow Edit Profile	Specifies whether the ACU can be used to edit the client adapter configuration profile. <b>Range:</b> yes or no <b>Default:</b> yes
Allow Export Profile	Specifies whether the ACU can be used to export the client adapter configuration profile to a disk file. <b>Range:</b> yes or no <b>Default:</b> yes
Allow Edit WEP	Specifies whether the ACU can be used to edit the WEP security options in the client adapter configuration profile. <b>Range:</b> yes or no <b>Default:</b> yes

## Auto Profile Selection

When Auto Profile Selection is selected in the Profile field, you can manage up to 16 profiles (or saved configurations) for a client adapter. These profiles enable the client adapter to be used in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using the client adapter at the office, at home, and in public areas such as airports. After the profiles are created, they are automatically switched without requiring you to reconfigure the client adapter each time it is moved to a new location.



### Note

Auto profile selection does not support profiles with multiple SSIDs, profiles with a null SSID (no value specified), or profiles with the same SSID.

## Profiles Tab

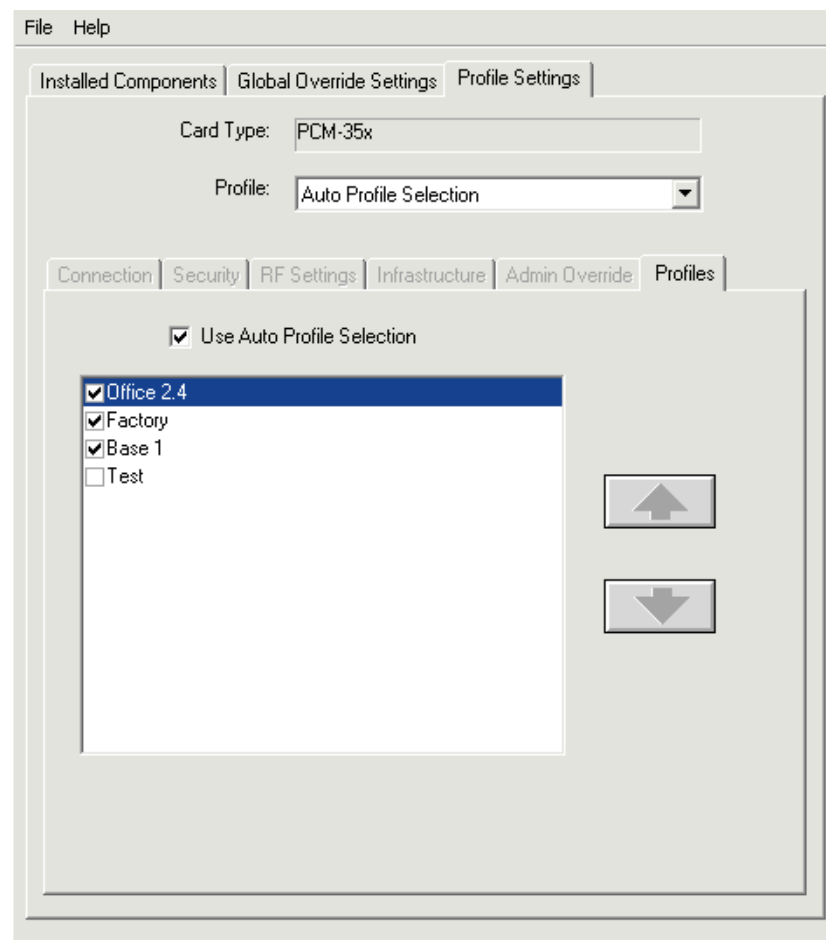
When you select Auto Profile Selection using the Profile drop-down menu, the Profiles tab window appears (see [Figure 4-13](#)). The window lists all available profiles and enables you to select and prioritize the profiles that are automatically switched. When you roam from one area to another, the SSIDs from the profiles are scanned by priority until a connection to an access point is established. When the client adapter's association to the access point is lost, the SSID scanning starts again from the highest priority profile in the list.



### Note

Auto profile selection does not display profiles containing a null SSID (no value specified), a duplicate SSID, or multiple SSIDs. These types of profiles cannot be used in auto profile switching.

**Figure 4-13** Profile Tab Window



## Setting Priorities and Activating Auto Profile Selection

To set priorities and activate auto profile selection on the client adapter, follow these steps:

- 
- Step 1** Check the profiles that you want to include in auto profile selection.
  - Step 2** Click each profile and use the up and down arrow keys to position the profile into the desired order, highest priority at top of the list and the lowest priority at the bottom of the list.
  - Step 3** Check the **Use Auto Profile Selection** check box.
-