

Cisco Aironet Configuration Administration Tool

The new Cisco® Aironet® Configuration Administration Tool allows network administrators to automate the process of installing or upgrading Cisco Aironet wireless LAN client adapter software and profiles on hundreds or thousands of machines that run Windows 98, 2000, Me, NT, and XP. This document provides guidelines for using the new Cisco Aironet Configuration Administration Tool.

The new Cisco Aironet Configuration Administration Tool is the second-generation automated client installation and configuration utility tool from the Cisco Aironet Series. The first-generation tool was a utility program called the Cisco Wireless Utility Auto Installer. This first tool provided automated assistance with installing Cisco Aironet wireless LAN (WLAN) client adapter drivers and utilities using a text-based editor. It did not provide assistance for installing WLAN drivers.

The new Cisco Aironet Configuration Administration Tool provides several enhancements to the first-generation tool. This second-generation tool uses a GUI to install all WLAN drivers, firmware, utilities, and profiles onto client machines and client adapters. The network manager uses the Aironet Configuration Administration Tool to distribute specific WLAN client adapter configurations to multiple end users. This tool allows network managers to simplify and control the WLAN client adapter installation configuration and downloading process for their end users. This tool also enables an IT administrator to perform the following functions:

- Select the Cisco Aironet software components that will be installed or upgraded on user machines
- Specify what functions in those software components will be overridden, or made unavailable, to the user
- Create profiles for adapters
- Bundle profiles, overrides, and software components in a customized downloadable image for installation by the Cisco Aironet Client Adapter Installation Wizard



Prerequisites

All required client administration software is installed with the Cisco Aironet Configuration Administration Tool. The following prerequisites are required to use this tool.

- Access point requirements—Access points to which the client adapters may attempt to authenticate must use the following firmware versions:
 - Cisco Aironet 340 and 350 Series access points firmware version 11.23T or later
 - Cisco Aironet 1100 Series access point with Cisco IOS Software 12.2(4)JA or later
 - Cisco Aironet 1200 Series access point with Cisco IOS Software 12.2(8)JA or later
 - VxWorks-based Cisco Aironet 1200 Series access point firmware version 11.54T or later
- WLAN client adapter requirements:
 - A Windows-based machine running Windows 98, NT 4.0, Me, 2000, or XP must be available for both configuration and distribution of the Cisco Aironet Configuration Administration Tool.

Configuration Procedure

Downloading Software

The Cisco Aironet Configuration Administration Tool and the latest Cisco Aironet Client Adapter Installation Wizard must both be downloaded on to the administrator's machine. These files are available for download from the Cisco Wireless Software Center on Cisco.com. All necessary WLAN client adapter files (drivers, firmware, and utilities) are included in the Cisco Aironet Client Adapter Installation Wizard file. Windows users no longer need to download several individual files or bundles that previously required the separate extraction and installation of each file. The wizard file simplifies WLAN client adapter installation. The wizard file can be used with or without the Cisco Aironet Configuration Administration Tool.

File Structure of Downloaded Files

Once downloaded, unzip the Cisco Aironet Configuration Administration Tool and Cisco Aironet Client Adapter Installation Wizard files into separate folders. The unzipped wizard file will have a file structure similar to that displayed in Figure 1. The unzipped Cisco Aironet Configuration Administration Tool file will have a file structure similar to that displayed in Figure 2.



Figure 1 Cisco Aironet Client Adapter Installation Wizard File Structure

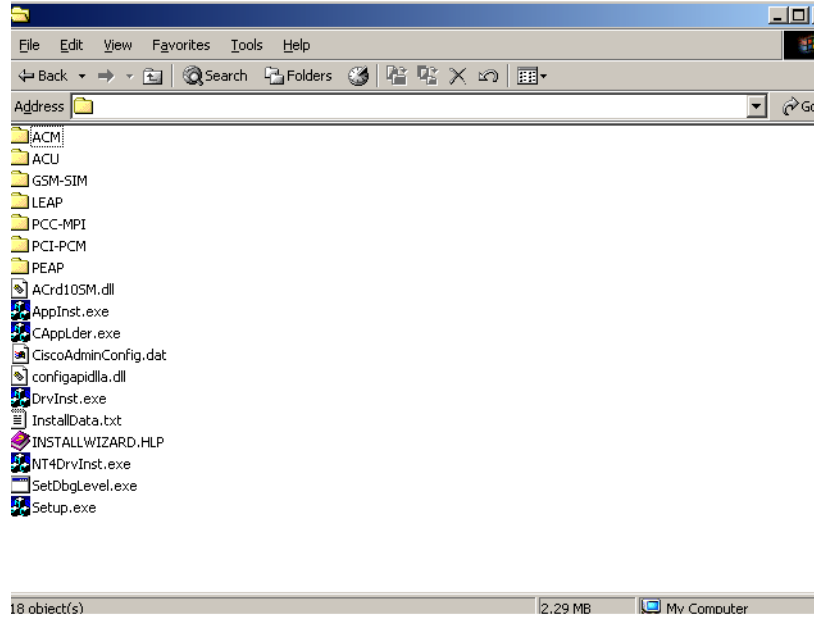
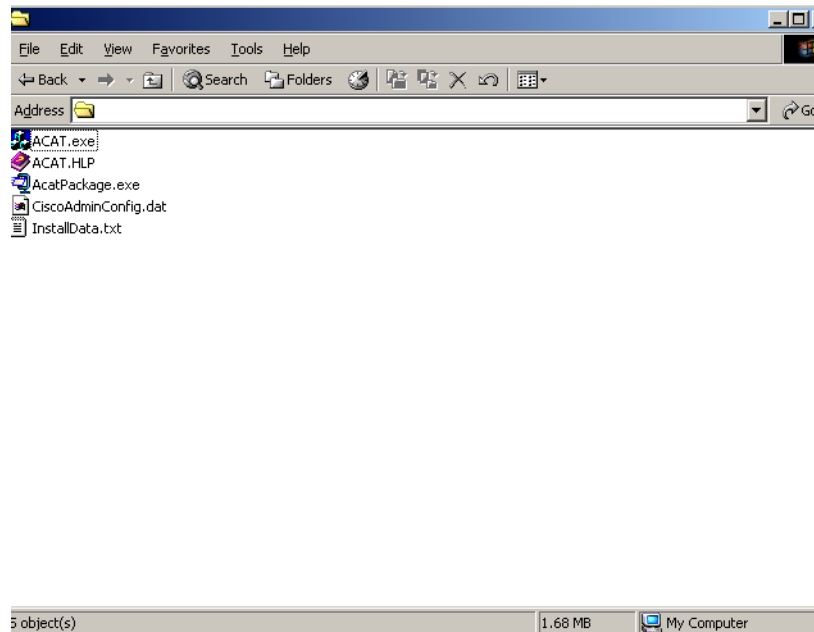


Figure 2 Cisco Aironet Configuration Administration Tool File Structure



Both folders contain a CiscoAdminConfig.dat file. This file is the key to the capability of the Cisco Aironet Configuration Administration Tool and the installation wizard. This file is encrypted and can only be read using the Cisco Aironet Configuration Administration Tool.



Note: Because the Cisco Aironet Configuration Administration Tool is freely downloadable by any knowledgeable end user, do not put security codes such as Wired Equivalent Privacy (WEP) keys inside the tool unless the file is protected to prevent it from being downloaded by unintended users. It is recommended that users be prevented from downloading the installation wizard; instead they should run the wizard directly from a network drive to protect all data.

Cisco Aironet Client Adapter Installation Wizard Details

The Cisco Aironet Client Adapter Installation Wizard automated installation program installs four primary components. Each of these components can be customized using the Cisco Aironet Configuration Administration Tool. These components include:

- *Radio firmware*—This software is copied into NVRAM on the client radio and will cause a momentary disruption in network connectivity while being installed. The radio firmware is specific to each individual radio type such as the Cisco Aironet 350 Series WLAN client adapters or Cisco Aironet 5 GHz 54 Mbps WLAN client adapter. The radio firmware is not transferable.
- *Windows drivers*—Also known as the network driver interface specification (NDIS) drivers. This software includes the drivers needed to interface between the radio card and the Windows OS. These drivers are OS-specific. Some NDIS drivers support multiple OSs in the same driver file.
- *Cisco Aironet Client Utility*—This utility software is the main interface between the client radio and the wireless network. This utility is used to configure the client security types, the identifying network name, or Service Set Identifiers (SSIDs). It allows users to manage their radio configuration. All Windows OSs and radio types use the same Cisco Aironet Client Utility file.
- *Cisco Aironet Client Monitor*—This new utility was introduced in conjunction with the Cisco Aironet Client Adapter Installation Wizard files. It is an optional application that runs “behind” a system tray icon and provides a subset of Cisco Aironet Client Utility features. The Cisco Aironet Client Monitor enables access to status information about the client adapter and simplifies basic tasks such as selecting a profile. It has three GUI components: an icon, a tool-tip window, and a pop-up menu. The Cisco Aironet Client Monitor is compliant with all Windows OSs and all radio types.

Read more about Cisco Aironet Client Adapter Installation Wizard files in the [Release Notes](#).

Cisco Aironet Configuration Administration Tool Details

The Cisco Aironet Configuration Administration Tool allows an administrator to create a customized CiscoAdminConfig.dat file. This customized file replaces the default CiscoAdminConfig.dat file placed inside the main installation folder during installation. As this placement occurs, the main installation folder is zipped and made into a self-executing.zip file.

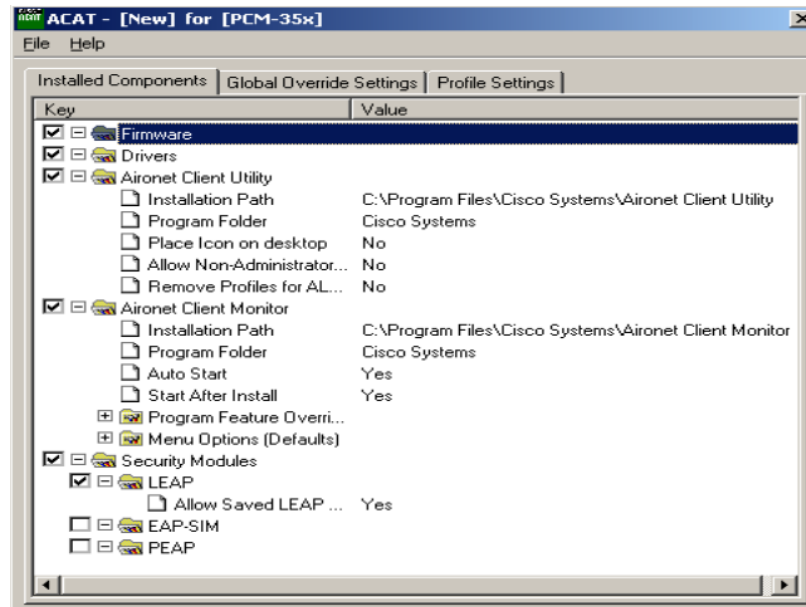
By replacing the default CiscoAdminConfig.dat file, the network administrator can define specific software, installation, and default parameters for client machines. A new CiscoAdminConfig.dat file must be created based on each client adapter radio type used within the WLAN installation—not based on the OS. An administrator may need to create up to nine installation .zip files with each file unique to a specific radio type such as the Cisco Aironet 350 Series WLAN client adapter or the Cisco Aironet 5 GHz 54 Mbps WLAN client adapter. Network administrators and end users can identify their WLAN client adapter radio type by looking at their client card label or by referring to their manual for laptop-embedded WLAN client adapter cards.



Cisco Aironet Configuration Administration Tool Configuration Process

Open the ACAT.exe file located inside the Cisco Aironet Configuration Administration Tool folder to begin the configuration process. This file runs the tool's program. Once opened, this file will automatically open a main program window that looks like Figure 3.

Figure 3 Cisco Aironet Configuration Administration Tool Main Program Window



The top blue bar lists the default configuration. The standard default configuration is defined for the PCMCIA 350 Series WLAN client adapter, also called the PCMCIA 350 Series radio card. If you are not installing the PCMCIA 350 Series radio card you will need to change the configuration file. Change the configuration file by selecting File> New> and then selecting the type of radio card for the configuration file that you are creating. The saved file name must be saved and stored as a file with the exact name CiscoAdminConfig.dat. For easy tracking and management, create a different folder for each radio type.

Note: It is strongly recommended that network administrators create a copy of their existing set-up file before creating new CiscoAdminConfig.dat files. This is recommended because any changes made to the CiscoAdminConfig.dat files' settings will overwrite all settings in the Cisco Aironet Configuration Administration Tool. Create a copy of the CiscoAdminConfig.dat file by selecting File > New File. This copy will save all current set-up configurations, profiles, and installation options. This option is discussed in more detail in the Profile Settings section later in this document.



Choosing Components To Install Onto The Client Machine

The Cisco Aironet Configuration Administration Tool main program window as seen in Figure 3 identifies which components an administrator wants to install onto the client machine. To configure the options in this window, double click on the selected option line and a dialogue box will open to accept changes to the selected field.

Installed Components Settings

Following are the options available on the first tab of the Cisco Aironet Configuration Administration Tool main program window as shown in Figure 3.

Radio Firmware and Drivers Configuration Options

The first two options displayed are for radio firmware and drivers. These two options do not have pull-down menus. Instead, check or uncheck the box to install the new drivers and firmware or to bypass the installation. By default the box is checked. This instructs the Cisco Aironet Configuration Administration Tool to check driver and firmware revision numbers to help ensure the user has the latest version available from the installation wizard folder. If the driver and firmware versions on the user machine are the same version numbers as available in the installation wizard folder, the Cisco Aironet Configuration Administration Tool bypasses the driver and firmware installation. If the driver versions are different, the Cisco Aironet Configuration Administration Tool will install the latest version available.

When the firmware and driver installation boxes are unchecked, the Cisco Aironet Configuration Administration Tool does not check or install the current firmware and driver versions.

Cisco Aironet Client Utility Configuration Options

The Cisco Aironet Client Utility configuration options include:

- *Installation Path*—Choose this option to specify a location for the default installation file. Most network managers install files into the default folder.
- *Program Folder*—Use this option to identify the name of the program installation folder. This affects both the folder name inside the client's folder structure, and the folder name inside the start menu.
- *Place Icon on Desktop*—This specifies if an icon for the Cisco Aironet Client Utility is placed onto the desktop. The default is “No” because the Cisco Aironet Client Monitor, located in the system tray, provides a quick link to opening the Cisco Aironet Client Utility. Check this box to select “Yes” if you would like the Cisco Aironet Client Utility icon to be placed onto the desktop.
- *Allow Non-Administrators to Save Settings*—This setting protects configuration options from being modified by non-administrators. This setting is only applicable if the primary user of the machine is going to be a non-administrator or if this machine will be used by multiple users.
- *Remove Profiles for all Cisco Wireless Adapters*—This setting is used only if the network administrator needs to overwrite a profile that a user may have already created on his or her laptop. The default is set to overwrite profiles with names identical to those created by the network administrator. This feature is discussed in more detail under the Profiles Setting section in this document. Please use care when setting this as a “Yes” option. There are no undo or retrieval options to recover removed client profiles once this program has been run on a client machine.



Cisco Aironet Client Monitor Configuration Options

The Cisco Aironet Client Monitor configuration options include:

- *Installation path*—Identical to the Cisco Aironet Client Utility. Please see the preceding explanation.
- *Program folder*—Identical to the Cisco Aironet Client Utility. Please see the preceding explanation.
- *Auto start*—This option specifies if the Cisco Aironet Client Monitor is loaded automatically upon boot-up.
- *Start after install*—This option specifies if the Cisco Aironet Client Monitor is opened immediately upon completion of the installation.
- *Program Feature Overrides versus Menu Options*—While the Program Feature Overrides and Menu Options may look identical, they are very different. Both options allow an administrator to modify the options available to users in the Cisco Aironet Client Monitor menu. However, if an administrator disables an item in the Program Feature Overrides, the user using the properties option cannot reselect that item. With Menu Options, items disabled by an administrator can be reenabled by a user if the user selects the properties menu and reselects the item. Therefore, the Program Feature Overrides provides the network administrator with additional controls and system security whereas the Menu Options is a convenience configuration option that provides the user with the flexibility to reenable properties that have been disabled by the network administrator.

Network Security Modules Configuration Options

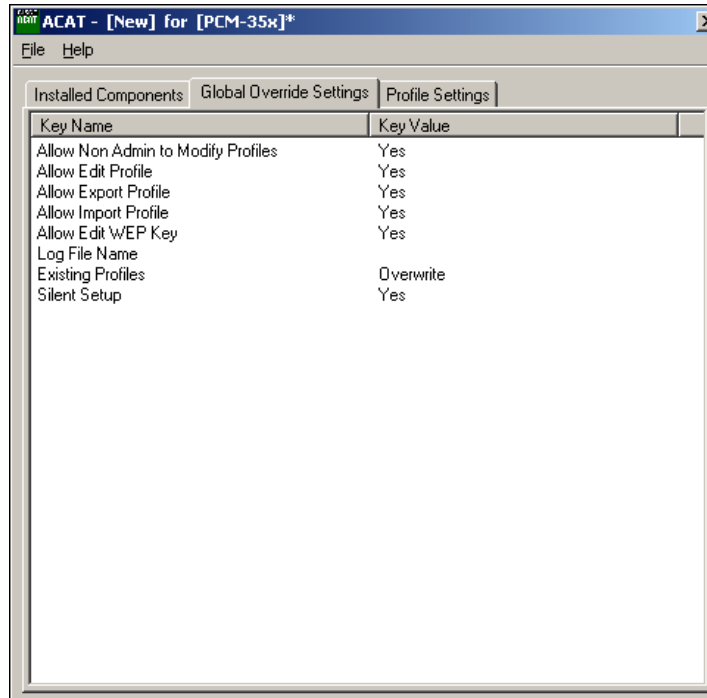
- *Cisco LEAP*—Select this option to install Cisco LEAP (an 802.1X Extensible Authentication Protocol [EAP] authentication type) capabilities onto the client machine. It is recommended that this option be selected if an administrator plans to run Cisco LEAP at any time in the future. Selecting this option during the initial installation saves time during future upgrades. The user configuration option included with Cisco LEAP allows users to save their username and password (encrypted in the registry) on their local machine.
- *EAP-Subscriber Identity Module (EAP-SIM)*—Select this option to install the 802.1X authentication type EAP-SIM onto the client machine.
- *Protected Extensible Authentication Protocol (PEAP)*—Select this option to install the 802.1X authentication type PEAP onto the client machine.



Global Override Settings

The next tab on the Cisco Aironet Configuration Administration Tool main program window (Figure 4) allows network administrators to set specific profile characteristics for the profiles created in the next session. Each of the following options can be changed via the user profile to create default options for each profile.

Figure 4 Global Override Settings



Key Name	Key Value
Allow Non Admin to Modify Profiles	Yes
Allow Edit Profile	Yes
Allow Export Profile	Yes
Allow Import Profile	Yes
Allow Edit WEP Key	Yes
Log File Name	
Existing Profiles	Overwrite
Silent Setup	Yes

- *Allow Non Admins to Modify Profiles*—This option ensures that standard and power users do not have the ability to change the profiles that administrators push out to users. This locks out the Cisco Aironet Client Utility from access by non-administrators. The word “Admins” is short for “Administrators.”
- *Allow Edit Profiles*—Very similar to the Allow Non Admins to Modify Profiles option except this option is for all users. Used by network security-conscious companies, this option specifies that profiles can only be configured by the Cisco Aironet Configuration Administration Tool, rather than locally by an individual user. Use caution when using this option because it makes troubleshooting difficult for local network administration personnel because it prohibits them from creating local configurations.
- *Allow Export Profiles*—Allows users to remove a profile from their local computer and share it with others. The profile is an encrypted file that cannot be read by users, but can be exported to other client computers.
- *Allow Import Profiles*—Allows a user to import another user’s profile. This is less of an information-security risk if the profile exporting options are disabled because it only allows users to share nonsecure profiles such as public-access or home-use profiles. Network-security profiles such as enterprise-campus or branch-office profiles can only be sent from one user to another if the Allow Export Profiles option is enabled.



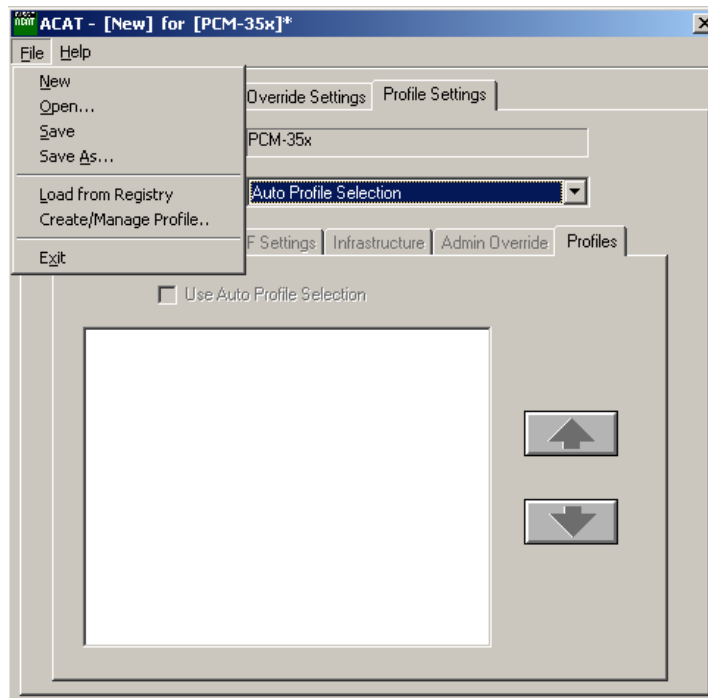
- *Allow Edit WEP Key*—This option is not an information-security concern because once a profile is created, the WEP key is hidden from users. However, this option does allow users to potentially break or corrupt their profiles. It also allows administrators to fix potential problems locally on the client's machine. If users have the ability to edit their WEP keys they have the ability to go into the Cisco Aironet Client Utility and change the WEP key. If users do not know the true WEP key they cannot set it back and would thus be prevented from accessing the network until an administrator manually inserted their WEP key, or reran the Cisco Aironet Configuration Administration Tool. It is safer to not allow users to change the WEP key.
- *Log File Name*—Allows administrators to create a log file name that suits their network environment.
- *Existing Profiles*—Use caution with this option. It allows an administrator to select the proper action to take when configuring a client machine. When “Yes” is selected for this option, all profiles, regardless of their use, are automatically deleted. Selecting “Yes” is not recommended because most users will set up additional profiles for their personal use at home or in public-access or hot spots. These users will not want their personal profiles to be deleted at every network-autogenerated profile update. Therefore, it is recommended that the default option called “Overwrite” be selected. This option overwrites only those profiles that have names identical to the profiles set up by the network administrator. All other profiles, including the user-defined profiles, are not changed. Another selection for this option is “Preserve.” Preserve does not delete any profiles; instead it defers to profiles created on the client's computer. The Overwrite option is the best choice for most installations because it allows administrators to continually update their company-specific profile and leave profiles created by end users intact. When using the Overwrite option, network administrators need to choose a unique name, not used by their end users, for their company profile file name.
- *Silent Setup*—This option allows the installation of the profile file to occur without generating end-user queries or requests for action.



Profile Settings

The final tab on the Cisco Aironet Configuration Administration Tool main program window (Figure 5) allows an administrator to create the client-machine profiles. A Cisco Aironet 350 Series PCMCIA client adapter card is used as an example in the following instructions. Network administrators need to create client-machine profiles specific to their Windows OS types and radio client cards. Each profile screen will look slightly different based upon the configurations for the specific OS, radio type, and other parameters.

Figure 5 Profile Settings Using Cisco Aironet 350 Series PCMCIA Client Adapter Card



Load from Registry Option

If an administrator has created the correct profiles and they are loaded on the administrator's machine, the administrator can use the "Load from Registry" shortcut available under File > Menu (Figure 5) to copy all the created profiles into the Cisco Aironet Configuration Administration Tool where they can be manipulated or saved into the CiscoAdminConfig.dat file.

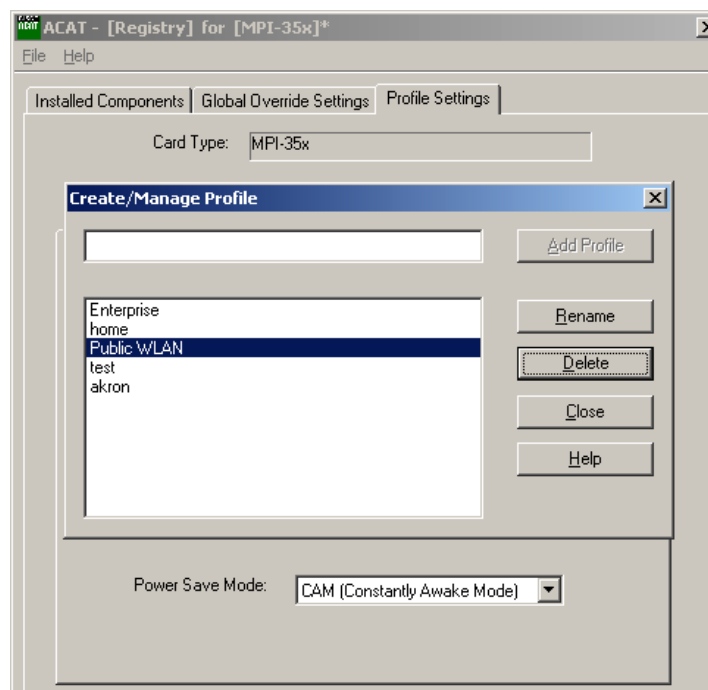
Note: When the Load from Registry shortcut is selected it will overwrite all options set in the other setting areas. Network administrators who want to use the Load from Registry shortcut are advised to select this option as their first step in creating the profiles—before making changes to any of the other Cisco Aironet Configuration Administration Tool settings.



Single or multiple profiles can be deleted within the Load from Registry setting by selecting the Create/Manage Profile option located under the File menu. This option is also used to create individual profiles that are not loaded from the registry. The Create/Manage Profile option does not reprompt to select the type of radio card for the profile. Instead, it uses the same radio card type as the most recently configured profile. If another radio card type is being configured, create a new file.

Created profiles can be renamed or deleted within this area via a pop-up screen (Figure 6) that automatically appears once profiles have been created. Once you have finished renaming or deleting the profiles, close this pop-up screen.

Figure 6 Profile Settings Management Screen



After the Create/Manage Profile screen has been closed, the main Profile Settings screen (Figure 5) will be activated and now contain the imported or created profiles from the Create/Manage Profile screen (Figure 6).

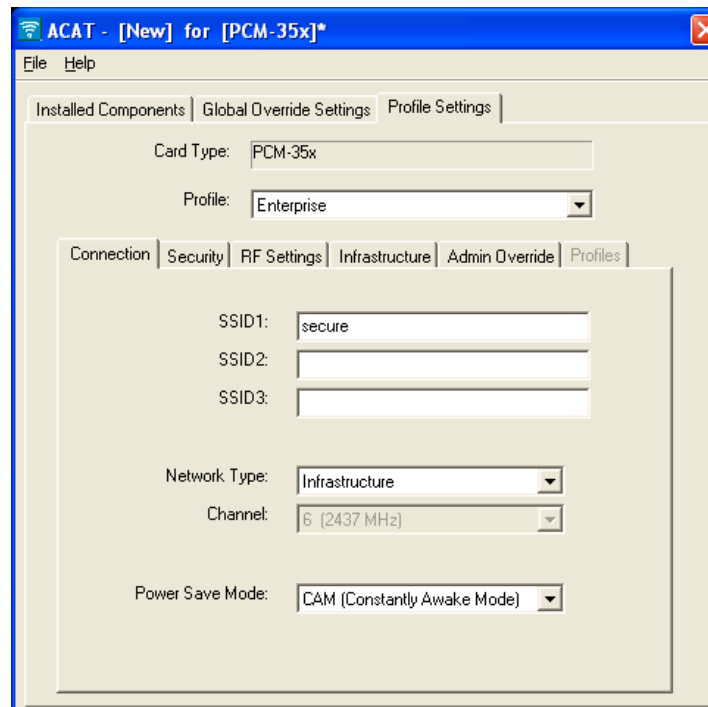
Note: The profile selection options cannot be changed for imported profiles. The profile tab under the Profile Settings will be grayed-out and not selectable for imported profiles.



Profile Settings Tabs

The options listed below are available within the Profile Settings option (Figure 7). These options are nearly identical to those on the Cisco Aironet Client Utility.

Figure 7 Profile Settings Options



- *Connection*—Allows an administrator to configure SSIDs and network type (Ad-Hoc vs. Infrastructure).
- *Security*—Allows selection of the profile security type. If the administrator did not select a profile security type at the first window (Installed Components), the Security option will not be available in the Security window. Under the WEP or 802.1X authentication setting there is a button that allows users to create specifics associated with each profile security type, such as the WEP key, or to save a username and password for 802.1X authentication.
- *RF Settings*—This is used for two very important options: transmit power and short-radio headers. If a client's computer, while in a selected profile, will never leave a specific environment, where all the access points are set to low power, the client transmit power can be lowered via the transmit power setting to reduce interference. For instance, at Cisco Systems®, all worldwide Cisco Aironet access points are set at 20mW or lower transmit power to reduce interference. Using this example, it might be beneficial for administrators to modify the Cisco Aironet client adapter transmit power of their enterprise profile to 20mW versus 100mW. Once 802.11h is ratified this will not be necessary because resetting of radio transmit power to reduce interference is part of the 802.11h specification and transmit power reduction will happen automatically. The use of short-radio headers is "on" by default but should be disabled when access points other than Cisco access points are used in the WLAN environment.

- **Infrastructure**—Most options on this screen are not commonly used except for two specific settings: Periodically Scan for Better Access Point and World Mode. In default mode of the Periodically Scan for Better Access Point option, clients will not roam to a new access point until five to seven access point beacons are lost. This might mean that a client has moved directly below a new access point but because it still has a weak but stable link to the former access point it will not roam. The Periodically Scan for Better Access Point option forces the client adapter to periodically poll all access points in close proximity and choose the one with the lowest number of clients and the best signal strength. In some unique cases, clients may bounce between access points more often, so please use this option with care. World Mode enables clients to automatically acquire certain settings such as transmit powers and allowable radio channels that are allowed in different countries. World Mode is recommended for both access points and clients to keep all clients compliant with the local country's wireless codes and regulations.
- **Admin Override**—The options on this screen are nearly identical to Global Override Settings, except that the setting changes on this screen apply only to selected profiles. All settings selected on this screen will override any Global Override Settings set on the Global Override Settings screen. The capability of the Admin Override settings, when applied to selected profiles, is identical to the capability of the Global Override Settings. Please read the Global Override Settings section of this document for details on individual option functions.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)