

# User's Guide for 802.11g Radios from Summit Data Communications, Inc.

Software Version 1.03

## Table of Contents

### [1.0 Introduction](#)

[1.1 Product Overview](#)

[1.2 Security Capabilities](#)

### [2.0 Getting Started](#)

[2.1 Install the Summit Software](#)

[2.1.1 Windows CE or Windows Mobile](#)

[2.1.2 Windows XP](#)

[2.2 Install the Radio](#)

[2.3 Configure the Manner of Obtaining an IP Address](#)

[2.3.1 Windows CE or Windows Mobile](#)

[2.3.2 Windows XP](#)

[2.4 Connect to Your WLAN](#)

[2.4.1 Preferred Method: Use SCU](#)

[2.4.2 Alternative: Use Windows Zero Config](#)

[2.5 Interact with the Radio](#)

### [3.0 Using the Summit Client Utility](#)

[3.1 Initializing SCU](#)

[3.2 Main Window](#)

[3.3 Profile Window](#)

[3.3.1 EAP Credentials](#)

[3.3.2 Encryption](#)

[3.3.3 ThirdPartyConfig](#)

[3.3.4 EAP-FAST](#)

[3.4 Status Window](#)

[3.5 Diags Window](#)

[3.6 Global Window](#)

### [4.0 Using the Summit System Tray Icon](#)

### [Appendix: Regulatory Information](#)

---

## 1.0 Introduction

Thank you for choosing one of the following wireless LAN radio modules or cards from Summit Data Communications, Inc.:

- Compact flash: Module with antenna connectors (SDC-CF10G) or card with integrated antennas (SDC-CF20G)
- PCMCIA: Module with antenna connectors (SDC-PC10G) or card with integrated antennas (SDC-PC20G)
- Miniature compact flash: Module with antenna connectors (SDC-MCF10G)

Your Summit WLAN radio, or WLAN client adapter, enables a computing device to communicate to a computing network using the IEEE 802.11g and IEEE 802.11b protocols.

This manual is a user's guide for a Summit radio that is installed on a computing device that is running one of the following operating systems:

- Windows CE 4.2 or Pocket PC (Windows Mobile) 2003
- Windows CE 5.0, Windows Mobile 5.0, or Windows Mobile 6.0
- Windows XP Embedded or Windows XP standard

The hardware components and software for all Summit radios are the same. A 20G version is a 10G version with integrated antennas. A PCMCIA version is a CF version in a specially designed CF-to-PCMCIA carrier. The miniature CF version is essentially the CF version with a different layout and a different (Molex) connector. The software that Summit provides for its radios includes:

- A device driver for the operating system running on the computing device that uses the radio
- An integrated IEEE 802.1X supplicant that supports the highest level of standards-based WLAN security with a broad range of options
- The Summit Client Utility (SCU), a configuration, monitoring, and management application designed for Summit radios
- On Windows CE and Windows Mobile, a service that displays in the Windows System Tray an icon that provides a visual status for the Summit radio and enables the user to launch SCU by tapping the icon

Your Summit radio is Wi-Fi CERTIFIED® and certified for Version 3 of Cisco Compatible Extensions (CCX):

- Wi-Fi: The Wi-Fi Alliance certifies that Summit radios support 802.11b and 802.11g with WPA and WPA2, both Personal and Enterprise. The EAP type tested by the Wi-Fi Alliance was PEAP-MSCHAPv2. For details, visit the Wi-Fi Alliance Web site at <http://www.wi-fi.com>, click on the "Wi-Fi CERTIFIED® Products" link, and search for Summit Data Communications.
- CCX: Summit radios are certified to Version 3 of the CCX specification for application-specific devices (ASDs). For an overview of CCX, go to [http://www.cisco.com/web/partners/pr46/pr147/partners\\_pgm\\_concept\\_home.html](http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html). For details on the features in CCX V3 for ASDs, go to [http://www.cisco.com/warp/public/765/ccx/versions\\_and\\_features.shtml](http://www.cisco.com/warp/public/765/ccx/versions_and_features.shtml).

## 1.1 Product Overview

For an overview of Summit WLAN radios, go to <http://www.summitdatacom.com/product.htm>.

## 1.2 Security Capabilities

Summit radios typically are used in business-critical mobile devices that transmit sensitive information, such as inventory data and patient information, over the air that separates the mobile devices from the network. To protect transmitted data as well as the mobile devices and network infrastructure that transmit and receive the data, an organization's IT department often imposes on mobile devices the same strict security standards imposed on other client devices. Summit's integrated approach to security simplifies the task of enforcing a consistent security policy on all devices.

A foundational element of the IEEE 802.11i WLAN security standard is IEEE 802.1X, and a critical application on a mobile device is an 802.1X supplicant. Such a supplicant provides an interface between the radio and the operating system and supports the authentication and encryption elements required for 802.11i, also known as Wi-Fi Protected Access 2 or WPA2, as well as predecessors such as WPA and WEP. Summit software includes an integrated supplicant that supports a broad range of security capabilities, including:

- 802.1X authentication using pre-shared keys or an EAP type, required for WPA2 and WPA
- Data encryption and decryption using WPA2 AES, WPA TKIP, Cisco TKIP, or WEP

The following EAP types are supported by the Summit software integrated supplicant and can be configured in SCU:

- PEAP: Provides secure user authentication by using a TLS tunnel to encrypt EAP traffic. Two different inner methods are used with PEAP:
  - EAP-MSCHAPV2, resulting in PEAP-MSCHAP: This is appropriate for use against Windows Active Directory and domains
  - EAP-GTC, resulting in PEAP-GTC: This can be used for authentication with static (login) passwords against a variety of databases. It also can be used for authentication with one-time passwords (OTPs) against OTP databases such as SecureID. Because Summit software does not support session resume, the use of PEAP-GTC with OTPs is not recommended. When a client device is power-cycled, or when the radio roams from one AP to another, the user must re-enter the OTP.
- EAP-TLS: Provides secure user authentication by using a TLS tunnel to encrypt EAP traffic. Provides very strong security, but relies on client certificates for user authentication credentials.
- LEAP: Is an authentication method for use with Cisco WLAN access points. LEAP does not require the use of server or client certificates. LEAP supports Windows Active Directory and domains but requires the use of strong passwords to avoid a vulnerability to offline dictionary attacks.
- EAP-FAST: Is a successor to LEAP and does not require strong passwords to protect against offline dictionary attacks. Like LEAP, EAP-FAST does not require the use of server or client certificates and supports Windows Active Directory and domains. EAP-FAST requires the provisioning of a protected access credential (PAC). SCU supports PACs that are provisioned manually and stored on the client device; SCU also supports dynamic PAC provisioning.

PEAP and EAP-TLS require the use of Windows facilities for the configuration of digital certificates.

With each of the EAP types supported by SCU, if authentication credentials are not stored in the active configuration profile, then the user is prompted to enter those credentials the first time the radio tries to associate to an AP that supports 802.1X (EAP).

## 2.0 Getting Started

Before you can use a Summit radio, you or your device manufacturer must install Summit software and the radio in your computing device. If you are doing the software and hardware installation, then you will need the following:

- A mobile computing device:
  - With a compact flash (CF) Type I or Type II slot or a PCMCIA (PC Card) Type II slot
  - That runs an operating system supported by Summit software (see section 1.0)

- Summit software
- A Summit radio module or radio card
- For a 10G Series radio module, one or two antennas, each with a cable that is fitted with a Hirose U.FL connector that can be attached to an antenna connector on the radio module

It is recommended that you install the software before you install the hardware. If you insert the card in your device before you install the software, then the "Found New Hardware Wizard" screen will appear, and you must select "Cancel" to cancel the Hardware Wizard.

## **2.1 Install the Summit Software**

### ***2.1.1 Windows CE or Windows Mobile***

Summit software for CE/Mobile is in a *.cab* file, which is the software equivalent of a "file cabinet". A Summit *.cab* file contains all software components, including the device driver and the Summit Client Utility (SCU). To install the Summit software, perform these tasks:

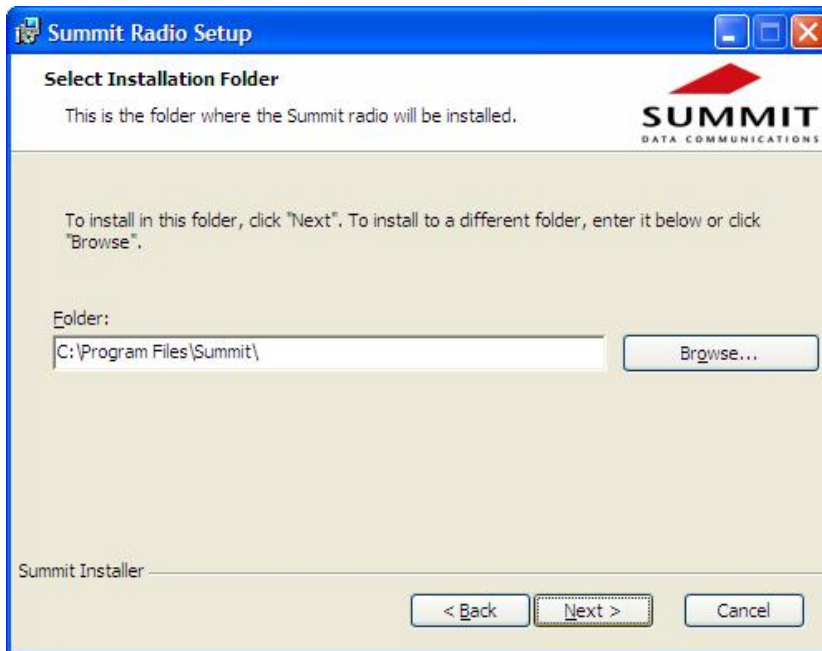
- Download the appropriate *.cab* file for the operating system and processor of your device. You can obtain your device's operating system and processor from the system information under Windows Control Panel (Tap Start, then Settings, and then System or Control Panel)
  - Pocket PC or Mobile: Select a *.cab* file with a name that begins with "mobile".
  - CE .NET: Do a search on your device's processor to determine if it is an ARM v4i processor or an ARM v4 processor. If it is an ARM v4i processor, select a *.cab* file with a name that begins with "sdc\_armv4i". If it is an ARM v4 processor, select a *.cab* file with a name that begins with "sdc\_armv4".
- Copy the file to your device using a supported file transfer mechanism. Common methods of moving the file include:
  - Place the file on a supported Compact Flash or SD memory card and use that card for copying the file to the device.
  - Use a program such as FTP or Microsoft ActiveSync.
- On the device, use the resident File Explorer program to locate the *.cab* file.
- Run the *.cab* file by single-clicking the file or by right-clicking and selecting "run".
- If asked to replace any existing files on the device, answer "Yes to all".

### ***2.1.2 Windows XP***

On Windows XP, the process for installing Summit software is managed by a setup wizard named *SummitInstall.msi*. When you run this program, a sequence of screens guides you through the installation process.

After you click the Next button on the initial welcome screen, you advance to a screen, shown on the next page, on which you specify the folder in which Summit software will be installed. Once you click the Next button on this screen, you advance to a third screen where you click the Install button to complete the installation process.

You can use the same setup wizard to uninstall or upgrade Summit software.



## 2.2 Install the Radio

Once you have installed the Summit software, you must install the Summit radio in a CF or PCMCIA slot. To install a 20G Series radio card, you simply insert the card in an external card slot. To install a 10G Series radio module, you must complete two types of connections:

- **Module to device:** When you slide the radio module into a CF or PCMCIA slot, a connector on the end of the module mates with a connector on the device.
- **Antenna(s) to module:** To connect one or two antennas to the radio module, you use an antenna cable that mates with the antenna on one end and with the radio module's U.FL connector on the other end.

The standard approach is to install the module in the device first and then connect the antenna(s). If the antenna connectors on the radio module are not visible when the module is installed, however, then you will need to connect the antenna(s) before installing the module in the slot.

On Windows XP, when you insert the radio module or card into a CF or PCMCIA slot on the device for the first time, the operating system will recognize that a new hardware device is being installed and display a series of screens so that you can associate a device driver to that device. On the initial screen, select "No, not this time" for the question on whether or not Windows should connect to Windows Update to search for the driver. On the next screen, you can choose to install the software automatically. Windows will locate the driver and begin to install it.

Because the Summit driver has not been signed as a part of Windows Logo (also known as WHQL) testing, Windows displays a warning message, shown on the next page, when it starts to install the driver. Tap or click the "Continue Anyway" button so that Windows continues with driver installation.

To connect the antennas, take each antenna and its cable, which is fitted with a Hirose U.FL connector, and attach the antenna cable to the radio module by mating the U.FL connector on the antenna cable with a U.FL connector on the radio module. Connect the primary (or only) antenna to the main connector,

which is located nearer to the right edge of the module. If there is a second antenna, connect it to the auxiliary antenna connector, which is located nearer to the left edge of the module.

## **2.3 Configure the Manner of Obtaining an IP Address**

### ***2.3.1 Windows CE or Windows Mobile***

Here are the steps required to use facilities on Windows CE or Windows Mobile to configure the manner of obtaining an IP address:

- Select Programs, then Settings, then the Connections tab at the bottom of the Settings screen
- Select Connections and then Advanced
- On the Advanced Connections screen, select the Network Card button and then select the Summit WLAN Adapter from the list of available network devices
- On the screen that appears, choose that a server will assign an IP address (using DHCP) or enter a specific IP address
- If you select the Name Servers tab, you can statically configure DNS servers, but if you use DHCP for IP address assignment then DNS usually is supplied by the same server that hands out IP addresses

### ***2.3.2 Windows XP***

Here are the steps required to use facilities on Windows XP to configure the manner of obtaining an IP address:

- From the Start Menu, select Control Panel, then Network Connections
- From the list of network adapters, select the Wireless Network Connection with the Summit device name
- Select File, then Properties
- Scroll down to select Internet Protocol (TCP/IP), then Properties
- On the screen that appears, choose that a server will assign an IP address (using DHCP) or enter a specific IP address

You can configure DNS servers statically, but if you use DHCP for IP address assignment then DNS usually is supplied by the same server that assigns IP addresses.

## **2.4 Connect to Your WLAN**

Two methods exist for configuring the radio for operation on a wireless network. The first and preferred method is to use SCU, which is described in detail in the next section of this guide. The other method is to use WZC, which is the Microsoft program for configuring any WLAN card.

### ***2.4.1 Preferred Method: Use SCU***

To use SCU to connect to your wireless network, first initialize SCU (see Section 3.1) and go to the Profile window by tapping the Profile tab. The Default configuration profile, if not modified, does not

specify an SSID, an EAP type, or a method of data encryption. As a result, if the Default profile is the active profile, then the radio will associate only to an access point that broadcasts its SSID and requires no EAP type and no encryption. If no profile has been created for the WLAN to which you want to connect, then use the following steps to create and select a profile for your WLAN:

- Go to the Main window by tapping the Main tab.
- Tap the Admin Login button to have privileges to make changes to profiles. The default password is “SUMMIT”. If your administrator has changed that password, then you must ask your administrator for assistance in creating a profile for your WLAN.
- Go to the Profile window by tapping the Profile tab.
- Tap the New button. When a pop-up screen prompts for a name, enter any alpha-numeric name to identify this profile (as unique from other profiles that are defined).
- Tap the OK button to return to the Profile tab.
- Tap the Commit button to save the profile name.
- When a message pops up to indicate that this command has been saved, select OK on that pop-up to return to the Profile window.
- To configure the SSID for the network to which you wish to associate, enter an SSID in the text box to the right of “SSID”, and select the Commit button and OK at the pop-up.
- To configure authentication and encryption, use the appropriate drop-down boxes on the window, and enter credentials for IEEE 802.1X EAP types or WEP keys just below the drop-down boxes. (To view the security drop-down boxes, you may have to minimize the alpha-numeric keyboard provided by the operating system.)
- Configure any other settings that are dictated by the network administrator for the SSID to which you must associate, being sure to tap Commit after you configure all settings.
- Tap the Main tab. In the Active Profile drop-down box will appear the newly created profile. Select this profile, and the Summit radio will attempt to connect to the network using the following steps:
  - Associate to the SSID
  - Authenticate to the network
  - If EAP authentication is being used, derive dynamic encryption keys
  - If DHCP is being used by the network, obtain an IP address

To assist with troubleshooting of any connectivity issues, the Status window reflects the current state of the device and the Diag window allows for DHCP renewal and ICMP Echo Requests, also known as Pings, to be sent by the device. You can learn more about using these SCU windows in Section 3.

#### ***2.4.2 Alternative: Use Windows Zero Config***

Another method of configuring the radio is through the operating system’s WZC feature. If the radio is inserted and the SCU is not configured, then WZC will attempt to use the card to attach to an available WLAN. A pop-up box will appear that indicates which networks (SSIDs) have been located and asks the user which network the device should use. Selecting an SSID that requires security will prompt the user for security keys or credentials. If the correct credentials are entered, then the WZC process will attempt to associate, authenticate, and run the appropriate encryption required to connect the user to the network.

If you want the Summit radio in your client device to connect not to a WLAN infrastructure but to a WLAN radio in another client device using ad hoc (or peer-to-peer) mode, then WZC is your only option. Ad hoc mode is not supported by SCU.

## **2.5 Interact with the Radio**

You can configure radio and security settings, monitor performance and activity, and troubleshoot issues with the radio using any of the following:

- SCU
- Another application, such as Wavelink Avalanche, that uses the application programming interface (API) for SCU
- Native facilities in the operating system, such as WZC

The rest of this guide assumes that you are using SCU for all interactions with the radio.

### **3.0 Using the Summit Client Utility**

The Summit Client Utility (SCU) is an application designed for end users and administrators of mobile devices that use a Summit radio. Using SCU, an end user can:

- Disable the radio (turn it off) and enable the radio (turn it on)
- View the contents of configuration profiles, or profiles, each of which houses the RF, security, and other settings for the radio
- Select the profile to be used
- View global settings, which apply to every profile or to SCU itself
- View a snapshot status of the current wireless network connection
- View more detailed status information on the radio, the AP to which it is connected, and the RF connection or link between the two
- View in-depth diagnostic information on the connection and the radio, most likely to report it to an administrator when there is a connection or performance issue
- Perform various troubleshooting and diagnostic tests
- View other information on the radio, such as software versions and regulatory domain

After completing an administrator login to the utility, a user can perform these additional tasks:

- Create, rename, edit, and delete profiles
- Alter global settings, which apply to every profile or to SCU itself

The SCU provides a graphical user interface (GUI) for access to all of its functions. Access to these functions also is available through an application programming interface (API) that is defined in a software developer's kit (SDK). Through the API, an application such as Wavelink Avalanche can manage Summit radios.

#### **3.1 Initializing SCU**

To initialize SCU on Windows CE or Mobile:

- From the Start menu, select Programs.
- Select the directory called Summit.
- Inside the Summit directory are two items: a directory for the storage of security certificates and the SCU. To run SCU, double-click the SCU icon.

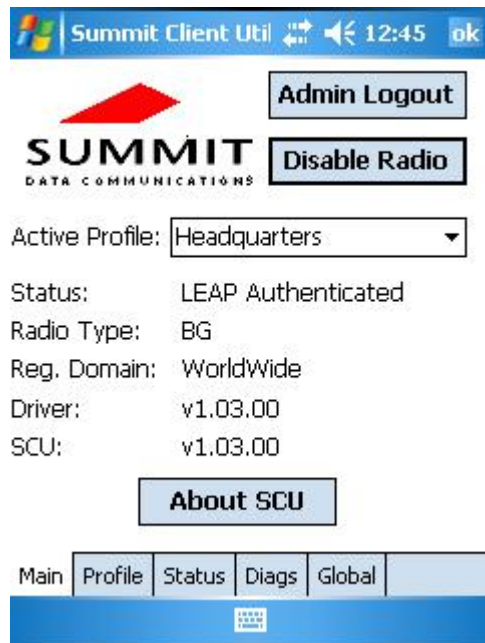
To initialize SCU on Windows XP, go to the Start menu, locate the SCU icon, and click it.

SCU has five windows: Main, Profile, Status, Diags (or Troubleshooting), and Global. SCU displays one tab for each window. To view a window, simply tap its tab. Each window is described in more detail in this section.

### 3.2 Main Window

Figure 1 on the next page is an example of a Main window. Here are the highlights of the Main window, beginning at the top of the window:

- **Admin Login/Logout button:** To login to SCU as an administrator, you select this button when “Admin Login” is displayed and supply the correct admin password on the dialog box. The default password is “SUMMIT” in all capital letters. (The password can be changed through the Admin Password function on the Global window.) Once you are logged in as an administrator, tapping the button again logs you out as an administrator, leaving you with access only to end-user functions.
- **Enable/Disable Radio button:** When the radio is enabled, selecting this button disables it; when the radio is disabled, selecting this button enables it.
- **Active Profile:** A user can view the name of the active profile and use the selection list to select a different profile. If “ThirdPartyConfig” is selected then, after the device goes through a power cycle, WZC or another application is used for configuration of the SSID, Auth Type, EAP Type, and Encryption settings.



**Figure 1: Main Window**

- **Status:** Indicates if the radio is associated to an access point and, if not, what the radio’s status is. Potential values are: Down (not recognized), Disabled, Not Associated, Associated, or [EAP type] Authenticated.
- **Radio Type:** Indicates the type of radio in the device. “BG” means a Summit radio that supports 802.11b and 802.11g.

- **Regulatory domain:** Indicates the regulatory domain or domains for which the radio is configured. “Worldwide” means that the radio can be used in any domain. The domain cannot be configured by an administrator or user.
- **Driver:** Indicates the version of the device driver that is running on the device.
- **SCU:** Indicates the version of SCU that is running on the device. (Displayed if space permits.)
- **About SCU:** When tapped, supplies information on SCU that on a Windows application normally would appear under Help > About, including driver and SCU version.

### 3.3 Profile Window

Profile settings are radio and security settings that are stored in the registry as part of a configuration profile. When a profile is selected as the active profile on the Main window, the settings for that profile become active. When the profile named ThirdPartyConfig is selected, a power cycle also must be performed.

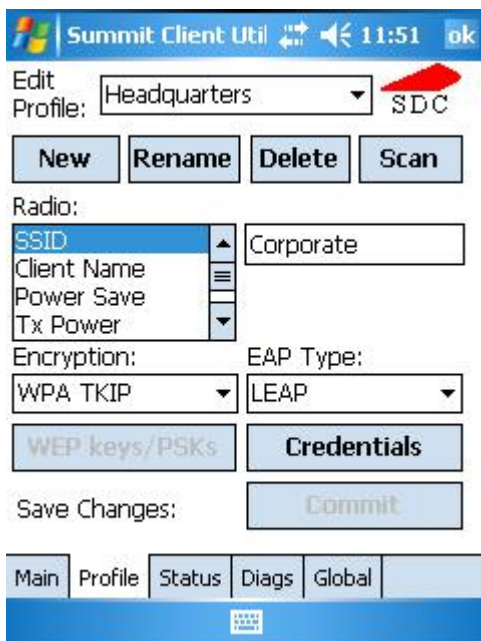
If it is not modified, then the Default profile does not specify an SSID, an EAP type, or a method of data encryption. As a result, if the Default profile is the active profile, then the radio will associate only to an access point that broadcasts its SSID and requires no EAP type and no encryption.

On the Profile window, an administrator can:

- Define up to 20 profiles, in addition to the special ThirdPartyConfig profile
- Change the settings in any profile
- Delete any profile except the special ThirdPartyConfig profile and the active profile

Profile changes made on the window are saved to the profile only when the Commit button is pressed.

Figure 2 below is an example of a Profile window:



**Figure 2: Profile Window**

Here are the highlights of the Profile window:

- **Edit Profile:** This is used to select the profile to be viewed or, if you are an administrator, edited.
- **Actions:** Four actions are available, with the first three available only to an administrator:
  - **New:** Create a new profile with default settings and give it a unique name, which is a string of up to 32 characters. You then can change the settings in the profile using other selections on the window.
  - **Rename:** Give the profile a new name, one that is not assigned to another profile.
  - **Delete:** Delete the profile, provided that it is not the active profile.
  - **Scan:** Open a window that lists access points that are broadcasting their SSIDs. Each time you tap the Refresh button, you view an updated list of APs, with each row showing an AP's SSID, its received signal strength indication (RSSI), and whether or not data encryption is in use (true or false). You can sort the list by clicking on the column headers. If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security. If you are authorized as an administrator and tap an SSID in the list, you return to the Profile window to create a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "\_1" if a profile with the SSID as its name exists already).
- **Radio:** Radio attributes in the list box on the left can be selected individually. When an attribute is selected, the current setting or an appropriate selection box with the current setting highlighted appears on the right.
- **Security:** Values for the two primary security attributes, EAP type and encryption type, are displayed in separate dropdown lists, with the current values highlighted. When you as an administrator select an EAP type, the Credentials button becomes active; when you tap it, a dialog box appears that enables you to define authentication credentials for that EAP type. When you as an administrator select an encryption type that requires the definition of WEP keys or a pre-shared key, the PSKs/WEP Keys button becomes active; when you tap it, a dialog box appears that enables you to define WEP keys or a PSK.
- **Save Changes:** To ensure that changes to profile settings made on the window are saved in the profile, you must tap the Commit button. If you make changes without tapping Commit and attempt to move to a different SCU window, SCU will display a warning message and give you the option of saving your changes before you leave the Profile window.

Here are the radio settings available on the Profile window:

- **SSID:** Service set identifier (SSID) for WLAN to which radio will connect
  - Value: A string of up to 32 characters
  - Default: None
- **Client Name:** Name assigned Summit radio and client device that uses it
  - Value: A string of up to 16 characters
  - Default: None
- **Power Save:** Power save mode for radio
  - Value:
    - CAM: Constantly awake mode
    - Maximum: Maximum power savings
    - Fast: Fast power save mode
  - Default: Fast
- **Tx Power:** Transmit power – Can be overridden by Cisco AP if CCX global setting is On and AP defines maximum transmit power for client as lower value
  - Value:

- Max: Maximum defined for current regulatory domain
    - One of the following values in milliwatts (mW): 50, 30, 20, 10, 5, 1
  - Default: Max
- **Bit Rate:** Bit rate used by radio when interacting with WLAN access point (AP)
  - Value: Auto (rate negotiated automatically with AP) or one of the following rates in megabits per second (Mbps): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 -- *If you select a particular bit rate, then the radio will not connect to an AP unless the specified SSID is configured for only the selected bit rate*
  - Default: Auto
- **Radio Mode:** Use of 802.11g and/or 802.11b when interacting with AP
  - Value:
    - B rates only: 1, 2, 5.5, and 11 Mbps
    - G rates only: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
    - BG rates full: All B and G rates
    - BG rates optimized: 1, 2, 5.5, 6, 11, 24, 36, and 54 Mbps -- *The "BG rates optimized" value is optimized for Cisco APs running IOS in autonomous mode (without controllers). This Radio Mode value is not optimized for Cisco APs that are tied to controllers. In fact, Summit recommends against using the "BG rates optimized" value when a Summit radio will associate with controller-based APs. An alternative to selecting a different value for Radio Mode is to set the 11 Mbps rate to "supported" instead of "mandatory" on each controller.*
  - Default: BG rates optimized
- **802.11 Auth:** 802.11 authentication type, used when associating to AP
  - Value: Open, shared-key, or LEAP (Network-EAP)
  - Default: Open

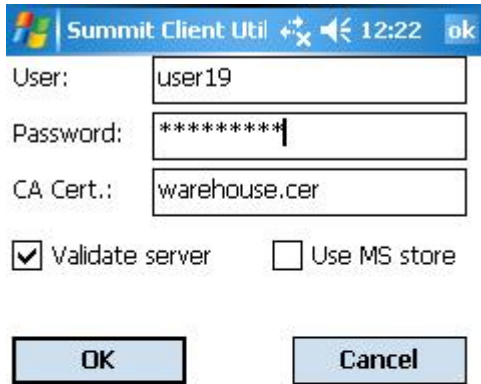
Here are the security settings available on the Profile window:

- **EAP type:** Extensible Authentication Protocol type used for 802.1X authentication to AP
  - Value: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, EAP-TLS
  - Default: None
- **Credentials:** Authentication credentials for the selected EAP type -- *See the section on **EAP Credentials** below the list.*
  - Values for LEAP:
    - User: Username or Domain\Username (up to 64 characters)
    - Password (up to 32 characters)
  - Values for EAP-FAST:
    - User: Username or Domain\Username (up to 64 characters)
    - Password (up to 32 characters)
    - PAC Filename (up to 32 characters)
    - PAC Password (up to 32 characters)
  - Values for PEAP-MSCHAP, PEAP-GTC, or EAP-TLS:
    - User: Username or Domain\Username (up to 64 characters)
    - Password (up to 32 characters)
    - "Validate server" checkbox: Check this if you are using a CA certificate to validate an authentication server. When this is checked, you must enter a certificate filename in the CA Cert field or check the "Use MS store" checkbox.
    - CA Cert: Filename of root certificate authority (CA) digital certificate (up to 32 characters) -- leave blank if "Use MS store" checkbox is checked

- "Use MS store" checkbox: Check this if the Microsoft certificate store should be used for a CA certificate. This is applicable only when "Validate server" is checked.
  - Additional values for EAP-TLS:
    - User Cert: Click the "..." button to select a user (or client) certificate from the Microsoft certificate store. You may not enter a filename, because the user certificate must reside in the Microsoft certificate store. When you browse for a certificate, the pop-up box shows two fields, Issued By and Issued To.
    - Priv. key pwd: Password for user certificate (up to 32 characters)
  - Defaults: None
- **Encryption:** Type of encryption (and decryption) used to protect transmitted data -- *See the section on **Encryption** below the list.*
  - Value:
    - **None:** No encryption
    - **Manual WEP:** WEP with up to four static keys -- 40-bit or 128-bit in ASCII or hex -- defined under WEP/PSK Keys
    - **Auto WEP:** WEP with key generated during EAP authentication
    - **WPA-PSK:** TKIP with PSK -- ASCII passphrase or hex PSK -- defined under WEP/PSK Keys
    - **WPA-TKIP:** TKIP with key generated during EAP authentication
    - **WPA2-PSK:** AES with PSK -- ASCII passphrase or hex PSK -- defined under WEP/PSK Keys
    - **WPA2-AES:** AES with key generated during EAP authentication
    - **CCKM-TKIP:** TKIP with key generated during EAP authentication and with Cisco key management protocol for fast reauthentication
    - **CKIP Manual:** WEP with up to four static keys-- 40-bit or 128-bit in ASCII or hex -- defined under WEP/PSK Keys, plus Cisco TKIP and/or Cisco MIC if configured on AP
    - **CKIP Auto:** WEP with key generated during EAP authentication, plus Cisco TKIP and/or Cisco MIC if configured on AP
  - Default: None

### 3.3.1 EAP Credentials

Figure 3 below is an example of a PEAP credentials window:



**Figure 3: PEAP Credentials Window**

The 802.1X authentication types PEAP and EAP-TLS rely upon information in digital certificates that are created by a certificate authority, or CA. To enable a client device to validate (or authenticate) the server used for PEAP or EAP-TLS authentication, you must provision a root CA certificate and distribute it to that client. You can store the CA certificate in a device's Microsoft certificate store or in a directory with a path that you specify as the value for Certs Path on the SCU Global window. If you don't specify a Certs Path value, then SCU uses for the Certs Path value the path to the certs directory that is off the SCU folder. For EAP-TLS you also must generate a user certificate for each client; that user certificate must be stored in the Microsoft certificate store on the client.

Instead of using digital certificates, EAP-FAST relies upon strong shared-secret keys that are unique to users. These secrets are called protected access credentials (PACs) and can be created automatically or manually. With automatic or in-band provisioning, the PAC is created and distributed to the client device in one operation. With manual or out-of-band provisioning, the PAC is created in one step and then must be distributed to the client device separately. SCU supports PACs created automatically or manually. When you create a PAC manually, you must load it to the directory identified by the Certs Path global setting. Be sure that the PAC file does not have read-only permissions set, or SCU will not be able to use the PAC.

Here are some important notes on entering credentials for EAP authentication:

- Any password provided for EAP authentication, whether in a profile or in an authentication dialog box, should not contain parentheses. Neither SCU nor the dialog box flags a parenthesis as an invalid character, but the integrated supplicant treats parentheses as delimiters and interprets the characters between a left parenthesis and a right parenthesis as the "true" password.
- If the credentials specified in the profile are incorrect then, when that profile is used, the authentication will fail without an error message, and the user will not be prompted to enter correct credentials
- If the credentials are not specified in the profile then, when the radio tries to associate using that profile, the user will be prompted to enter the credentials

- When prompted, the user can enter valid credentials, enter invalid credentials, or cancel the operation
  - If the user enters valid credentials and taps the OK button, the radio will associate and authenticate
  - If the user enters invalid credentials and taps the OK button, the radio will associate but not authenticate, and the user will be re-prompted to enter credentials
  - If the user taps the Cancel button or the user clears the credentials fields and taps the OK button, then the radio will not attempt to associate with that profile until the user performs one of the following actions (while the profile is the active profile):
    - Causes the device to go through a power cycle or suspend/resume
    - Disables and enables the radio or taps the Reconnect button on the Diags windows>
    - Modifies the profile and taps the Commit button

Alternatively, the user can select another profile as the active profile and then switch back to the profile for which EAP authentication was canceled.

### **3.3.2 Encryption**

#### **Cisco TKIP**

If the active profile has an Encryption setting of CKIP Manual or CKIP Auto, then the Summit radio will associate or roam successfully to an AP is configured with:

- The SSID and other RF settings of the active profile
- The authentication method of the active profile
- For Manual WEP, the static WEP keys of the active profile
- Any of the following encryption settings:
  - WEP only (no CKIP or CMIC)
  - WEP with CKIP
  - WEP with CMIC
  - WEP with CKIP and CMIC

#### **WPA Migration Mode and WPA2 Mixed Mode**

Summit radios support two special access point (AP) settings: WPA Migration Mode and WPA2 Mixed Mode. WPA Migration Mode is a setting on Cisco APs that enables both WPA and non-WPA clients to associate to an AP using the same SSID, provided that the AP is configured for Migration Mode (WPA optional with TKIP+WEP128 or TKIP+WEP40 cipher). In other words, WPA Migration Mode means WPA key management with TKIP for the pairwise cipher and TKIP, 128-bit WEP, or 40-bit WEP for the group cipher. When WPA Migration Mode in use, you can select WPA TKIP or Auto WEP for your Summit radio encryption type.

WPA2 Mixed Mode operation enables both WPA and WPA2 clients to associate to an AP using the same SSID. WPA2 Mixed Mode is defined by the Wi-Fi Alliance, and support for the feature is a part of Wi-Fi certification testing. When WPA2 Mixed Mode is configured, the AP advertises the encryption ciphers (TKIP, CCMP, other) that are available for use, and the client selects the encryption cipher it wants to use. In other words, WPA Mixed Mode means WPA key management with AES for the pairwise cipher and AES or TKIP for the group cipher. When WPA2 Mixed Mode in use, you can select WPA2 AES or WPA TKIP for your Summit radio encryption type.

### **3.3.3 ThirdPartyConfig**

If the profile named “ThirdPartyConfig” is selected as the active profile, then SCU works in tandem with WZC or another third-party application for configuration of all radio and security settings for the radio. The third-party application must be used to define the SSID, Auth Type, EAP Type, and Encryption settings. SCU can be used to define the Client Name, Power Save, Tx Power, Bit Rate, and Radio Mode settings. Those SCU profile settings, all SCU global settings, and the third-party application settings are applied to the radio when ThirdPartyConfig is selected as the active profile and a power cycle is performed.

On some devices that run Pocket PC or Windows Mobile, the radio will not associate if WPA with pre-shared keys, or WPA-PSK, is used with WZC. If that is the case for your device, then to use WPA-PSK you must use an SCU profile other than ThirdPartyConfig.

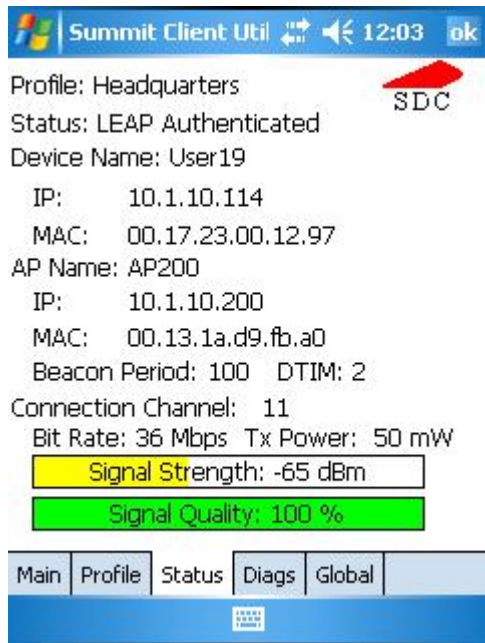
### **3.3.4 EAP-FAST**

The 802.1X authentication types PEAP and EAP-FAST use a client-server security architecture that encrypts EAP transactions within a TLS tunnel. PEAP relies on the provisioning and distribution of a digital certificate for the authentication server. With EAP-FAST, tunnel establishment is based upon strong shared-secret keys that are unique to users. These secrets are called protected access credentials (PACs) and can be created automatically or manually. With automatic or in-band provisioning, the PAC is created and distributed to the client device in one operation. With manual or out-of-band provisioning, the PAC is created in one step and then must be distributed to the client device separately.

SCU supports PACs created automatically or manually. When you create a PAC manually, you must load it to the *certs* directory on the device that runs SCU. Be sure that the PAC file does not have read-only permissions set, or SCU will not be able to use the PAC.

## **3.4 Status Window**

The Status window provides status information on the radio. A sample Status window is shown in Figure 4 below:



**Figure 4: Status Window**

Here is the information on the Status window:

- Name of active profile
- Association status -- Potential values are: Down (not recognized), Disabled, Not Associated, Associated, or [EAP type] Authenticated
- Information on the client device with the Summit radio
  - Client name, if defined in active profile
  - IP address
  - MAC address
- Information on access point to which Summit radio is associated
  - Name
  - IP address
  - MAC address
  - Beacon period: Amount of time between access point beacons in Kilomicroseconds, where one Kµsec equals 1,024 microseconds
  - DTIM interval: A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM), which tells power-save client devices that a packet is waiting for them (e.g. a DTIM interval of 3 means that every third beacon contains a DTIM)
- Information on WLAN connection between Summit radio and AP
  - Channel
  - Transmit power
  - Data (bit) rate
  - Signal strength (RSSI), displayed graphically and in dBm
  - Signal strength (%), a measure of the clarity of the signal, displayed graphically and in dBm

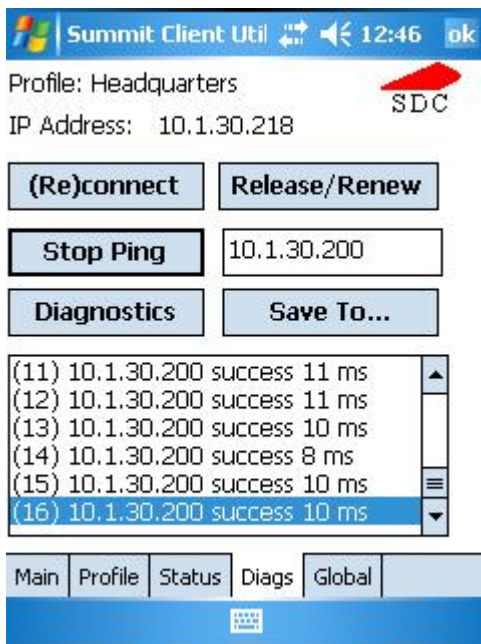
One status item, the radio association state, is shown on both the Status window and the Main window. A few status items are shown on the Main window and not the Status window. Those items are:

- SCU software version
- Driver software version
- Regulatory domain for radio: FCC, ETSI, TELEC, or Worldwide

When a ping initiated on the Diags window is active, the Status window displays a ping indicator consisting of two "lights" that alternative in "flashing" green (for a successful ping) or red (for an unsuccessful ping).

### 3.5 Diags Window

A sample Diags, or troubleshooting, window is shown in Figure 5 below:



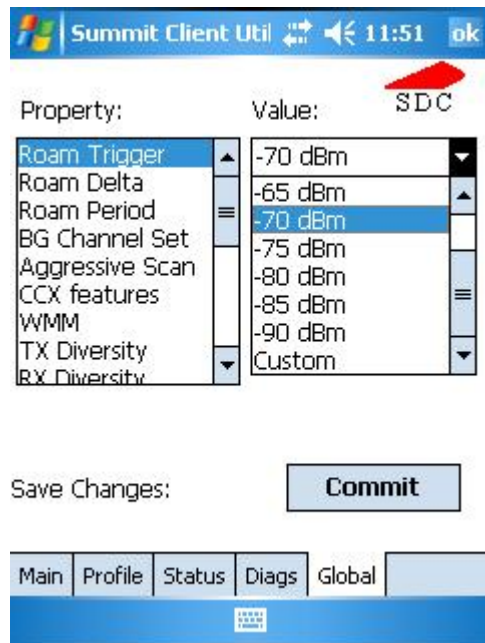
**Figure 5: Diags Window**

Here are the functions available on the Diags window:

- (Re)connect: Disable and enable the radio, apply or reapply the current profile, and attempt to associate and authenticate to the wireless LAN, logging all activity in the output area at the bottom.
- Release/Renew: Obtain a new IP address through DHCP release/renew, and log all activity in the output area at the bottom.
- Start Ping: Start a continuous ping to the address in the edit box next to the button. Once the button is tapped, its name and function will change to Stop Ping. Pings will continue until you tap the Stop Ping button, move to an SCU window other than Diags or Status, exit SCU, or remove the radio.
- Diagnostics: Attempt to (re)connect to an AP, and provide a more thorough dump of data than is obtained with (Re)connect. The dump will include radio state, profile settings, global settings, and a BSSID list of APs in the area.
- Save To...: Save the diagnostics output to a file.

### 3.6 Global Window

Global settings include radio and security settings that apply to all profiles and settings that apply to SCU itself. An administrator can define and change most global settings on the Global window in SCU. A sample Global window is shown in Figure 6 below:



**Figure 6: Global Window**

The following radio global settings, which apply to all configuration profiles, can be changed in SCU:

- **Roam Delta:** When Roam Trigger is met, second AP's signal strength (RSSI) must be **Roam Delta** dBm stronger than moving average RSSI for current AP before radio will attempt to roam to second AP
  - Value: 5, 10, 15, 20, 25, 30, 35, or Custom (see note on Custom below the list)
  - Default: 15
- **Roam Period:** After association or roam scan (with no roam), radio will collect RSSI scan data for **Roam Period** seconds before considering roaming
  - Value: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, or Custom (see note on Custom below the list)
  - Default: 10
- **Roam Trigger:** When moving average RSSI from current AP is weaker than **Roam Trigger**, radio does a roam scan where it probes for an AP with a signal that is at least Roam Delta dBm stronger
  - Value: -50, -55, -60, -65, -70, -75, -80, -85, -90, or Custom (see note on Custom below the list)
  - Default: -70
- **BG Channel Set:** Defines the 2.4 GHz channels to be scanned when the radio is contemplating a roam and needs to determine what APs are available.
  - Value: Full (all channels); 1,6,11 (the most commonly used 2.4 GHz channels); 1,7,13 (for ETSI and TELEC radios only); or Custom (see note on Custom below the list)
  - Default: Full

- **Aggressive Scan:** When this setting is On and the current connection to an AP becomes tenuous, the radio scans for available APs more aggressively. Aggressive scanning complements and works in conjunction with the standard scanning that is configured through the Roam Trigger, Roam Delta, and Roam Period settings. Summit recommends that the Aggressive Scan global setting be On unless there is significant co-channel interference because of overlapping coverage from APs that are on the same channel.
  - Value: On or Off
  - Default: On
- **CCX features:** Use of three CCX features -- AP-assisted roaming, AP-specified maximum transmit power, and radio management
  - Value: On, Off -- Note: Use "On" only when WLAN uses only Cisco APs
  - Default: Off
- **WMM:** Use of Wi-Fi Multimedia Extensions, also known as WMM
  - Value: On, Off
  - Default: Off
- **Frag Thresh:** If packet size (in bytes) exceeds threshold, then packet is fragmented
  - Value: An integer from 256 to 2346
  - Default: 2346
- **RTS Thresh:** Packet size above which RTS/CTS is required on link
  - Value: An integer from 0 to 2347
  - Default: 2347
- **RX Diversity:** How to handle antenna diversity when receiving data from AP
  - Value:
    - On-Start on Main: On startup use main antenna
    - On-Start on Aux: On startup, use auxiliary antenna
    - Main only: Use main antenna only
    - Aux only: Use auxiliary antenna only
  - Default: On-Start on Main
- **TX Diversity:** How to handle antenna diversity when transmitting data to AP
  - Value:
    - Main only: Use main antenna only
    - Aux only: Use auxiliary antenna only
    - On: Use diversity
  - Default: On
- **LED:** Use of LED; available only with MCF10G
  - Value: On, Off
  - Default: Off

If SCU displays a value of "Custom" for a global setting, then the operating system registry has been edited to include a value that is not available for selection on the Global window. Selecting "Custom" has no real effect. If SCU displays a value other than "Custom" and you select the value of "Custom" and tap the Commit button, then SCU reverts to the value that it displayed before you selected "Custom".

The following SCU global settings, which apply to SCU itself, can be changed in SCU:

- **Tray Icon:** Enabling of System Tray icon, which is described in detail on Section 4
  - Value: On, Off
  - Default: On
- **Hide Passwords:** If this is On, then SCU as well as EAP authentication dialog boxes mask passwords and other sensitive information, such as WEP keys

- Value: On, Off
  - Default: Off
- **Admin Password:** Password that must be specified when Admin Login button pressed
  - Value: A string of up to 64 characters
  - Default: SUMMIT
- **Certs Path:** Directory where certificate(s) for EAP authentication are housed
  - Value: A valid directory path of up to 64 characters
  - Default: Depends on device
- **Auth Timeout:** Specifies the number of seconds that Summit software will wait for an EAP authentication request to succeed or fail. If authentication credentials are specified in the active profile and the authentication times out, then association will fail. If authentication credentials are not specified in the active profile and the authentication times out, then the user will be re-prompted to enter authentication credentials
  - Value: An integer from 3 to 60
  - Default: 8
- **Ping Payload:** Amount of data in bytes to be transmitted on a ping
  - Value: 32, 64, 128, 256, 512, 1024
  - Default: 32
- **Ping Timeout ms:** Amount of time in milliseconds that transpires without a response before ping request is considered a failure
  - Value: An integer from 1 to 30000
  - Default: 5000
- **Ping Delay ms:** Amount of time in milliseconds between successive ping requests
  - Value: An integer from 0 to 7200000
  - Default: 1000

When a global setting is changed on the window and the Commit button is tapped, the change may not take effect until the device is power cycled. If you make changes without tapping Commit and attempt to move to a different SCU window, SCU will display a warning message and give you the option of saving your changes before you leave the Global window.

A few global settings can be defined or set only through a separate utility such as the Summit Manufacturing Utility, which Summit makes available only to device manufacturers and not to their customers.

## 4.0 Using the Summit System Tray Icon






On Windows CE and Windows Mobile, Summit software also includes a service that displays an icon in the Windows System Tray. That icon provides a visual status for the Summit radio in the device and enables the user to launch SCU by tapping the icon.

The software for the service is installed with other Summit software in a *.cab* file. The service is active and displays an icon in the System Tray only when all of the following are true:

- A Summit radio is installed in the device or inserted in an external slot in the device
- The device is active
- Windows Zero Config is **not** active
- The SCU Tray Icon global setting is On (the default setting)

Once the service is active, if you remove the radio, turn off the device, make WZC active, or set the Tray Icon global setting to Off (and power cycle the device), then the service is stopped and the tray icon removed.

When the service is active, it queries the driver every three seconds for the status of the connection for the active profile, as selected in the SCU Main window. Based on the driver's response to the query, the service displays one of the following icons:

-  The radio is not associated/authenticated to an access point (AP)
-  The signal strength (RSSI) for the current AP (to which the radio is associated) is -80 dBm or weaker
-  The RSSI for the current AP is stronger than -80 dBm but not stronger than -60 dBm
-  The RSSI for the current AP is stronger than -60 dBm but not stronger than -40 dBm
-  The RSSI for the current AP is stronger than -40 dBm

When you tap the icon, the SCU application is launched. On most CE devices, the System Tray icon is not visible while SCU is running, but the service remains active. If SCU usually runs on the device, or if you want to maximize performance, then you should disable the System Tray icon service by setting the Tray Icon global setting to Off and power cycling the device.

## Appendix: Regulatory Information

*Note: All declarations and instructions for the SDC-CF10G apply to other Summit 802.11g radio modules and cards.*

**Summit declares that SDC-CF10G (FCC ID: TWG-SDCCF10G) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.**

**This device is intended for host device manufacturers and integrators only under the following conditions:**

- 1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
- 2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as the two conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing its end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

**IMPORTANT NOTE:** In the event that the two conditions above cannot be met (for example certain device configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID cannot be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

- **End Product Labeling**

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users, for example, mobile data terminals (MDTs) and vehicle-mounted devices (VMDs). The final end product must be labeled in a visible area with the following: “Contains TX FCC ID: TWG-SDCCF10G”.

- **Manual Information That Must be Included**

The OEM integrator must not provide information to the end user regarding how to install or remove this RF module in the users manual of the end product which integrate this module.

The users manual for OEM integrators must include the following information in a prominent location “**IMPORTANT NOTE:** To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

**Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**IMPORTANT NOTE:**

**FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**Industry Canada (IC)**

This device has been designed to operate with the antennas listed below, and having a maximum gain of 0 dB. Antennas not included in this list or having a gain greater than 0 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication."

-----  
[1] See <http://www.cisco.com/warp/public/102/wlan/leapserver.html#NetEAP> for a Cisco explanation of 802.11 authentication using Open and Network-EAP. The Summit Client Utility refers to Network-EAP as "LEAP".

[2] See <http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12213ja/i12213sc/s13rf.htm#wp1044425>

[3] See <http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12213ja/i12213sc/s13rf.htm#wp1037656>

[4] The device manufacturer should use the Summit manufacturing utility to ensure that the "Tx Power" value reported by SCU is EIRP, or the total effective transmit power of the radio, including gains that the antenna provides and losses from the antenna cable.