Summit Client Utility

Administrator Guide
Version 1.0

global solutions: local support™
Americas : +1-800-492-2320 Option 3
Europe : +44-1628-858-940
Hong Kong : +852-2268-6567 x026
www.lairdtech.com/wireless

REVISION HISTORY

Revision	Date	Description
1.0	23 January 2015	Converted from HTML document.

CONTENTS

INTRODUCTION

This document is intended for administrators of mobile devices that use a Summit radio and Summit Software.

Note: For an overview of all Laird wireless LAN radios, refer to the Wi-Fi Products page of the website.

ACCESSING THE SUMMIT CLIENT UTILITY

The SCU is available for Windows Embedded CE, Windows Mobile, and Windows XP. Depending on your operating system, use one of the following methods to access SCU:

- Windows Embedded CE or Windows Mobile - From the Start menu, select **Programs > Summit > Summit Client Utility.**
- Windows XP - From the Start menu, select **All Programs > Summit > Summit Client Utility.**

Note: The Summit directory includes the SCU application and a directory for the optional storage of security certificates.

SCU has five tabbed windows which, depending on your operating system, may be accessed from the bottom of the screen (Windows CE or Windows Mobile) or from the top of the screen (Windows XP):

- Main Window
- Profile Window
- Status Window
- Diags Window
- Global Window

SUMMIT CLIENT UTILITY - ADMINISTRATOR FUNCTIONS

Main Window

The Main Window Provides an overview of the current wireless network connection configuration (Active Profile), a snapshot of connection information as well as access to administrator functions (Admin Login/Logout - *administrator use only*), and additional information regarding SCU (About SCU).

Figure 1 shows the SCU Main window in Windows CE/Windows Mobile and Windows XP operating systems.

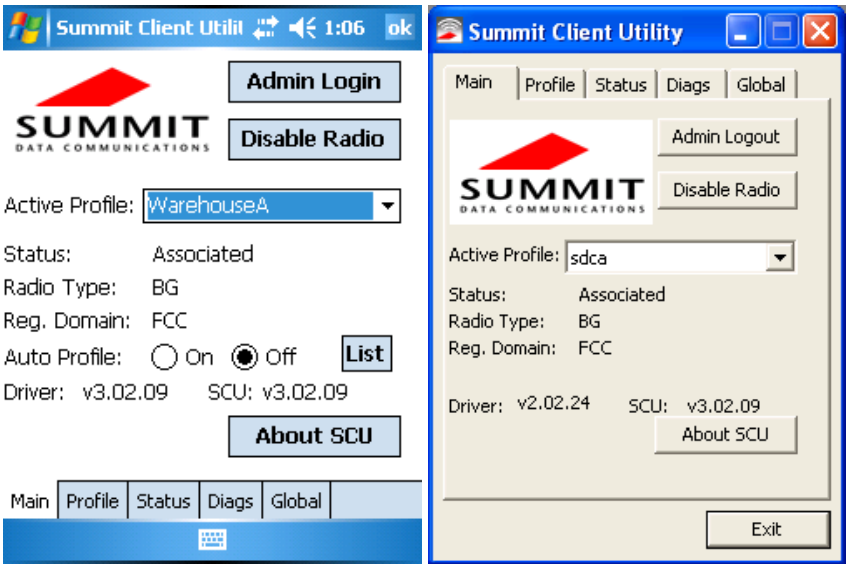


Figure 1: Main Window in Windows CE (left) and Windows XP (right)

The following are the SCU elements available from the Main Window:

- Admin Login/Logout
- Enable Radio/Disable Radio
- Active Profile
- Status
- Radio Type
- Reg. Domain
- Auto Profile
- Driver
- SCU
- Import/Export

Admin Login/Logout

To log in as an administrator, tap Admin Login and enter the administrator password in the dialog box. The default password is SUMMIT (case sensitive). Tap Admin Logout to log out as an administrator, leaving access to end-user functions only.

Note: The administrator password can be changed through the Admin Password function on the Global Window.

Enable Radio/Disable Radio

When the radio is enabled, select this button (which displays Disable Radio) to disable it. When the radio is disabled, select the same button (which now displays Enable Radio) to enable it. When disabled, the radio does not attempt to make a connection to an access point.

Active Profile

Displays the name of the active profile. Use the drop-down menu to select a different profile.

Note: If ThirdPartyConfig is selected (and after the device goes through a power cycle), WZC (Windows Zero Configuration) or another application is used to configure the SSID, Auth Type, EAP Type, and Encryption settings.

Note: When you use the drop-down to switch to a new active profile, a registry flush occurs of the entire Configs key and subkeys for the previous active profile.

Status

Indicates the current status of the Summit radio. Connection statuses include:

- Down - The radio is not recognized by Summit Software and therefore is not associated nor authenticated.
- Disabled - The radio is disabled. To enable the radio, tap Enable Radio located on the SCU Main Windows. When the radio is disabled, it does not attempt to make a connection to an access point.
- Not Associated - The radio has not established a connection to an access point.
- Associated - The radio has established a connection to an access point.
  - If the radio Encryption type is set to WEP or a pre-shared key (WPA-PSK or WPA2-PSK), it should not be capable of obtaining an IP address (either statically assigned or through DHCP) and passing traffic.
  - If the radio Encryption type requires EAP authentication then an EAP Type must be property configured in order for the device to obtain an IP address and be capable of passing traffic.
- <EAP Type> Authenticated - The radio has established a connection to an access point and has completed EAP Authentication successfully. If the radio is not sending or receiving data from the AP, one of the following may apply depending on the encryption method:
  - WEP: One of the WEP keys in the active profile is invalid.
  - WPA-PSK or WPA2-PSK: the PSK (password) is invalid.
  - WAP-Enterprise or WPA2-Enterprise: The radio did not complete EAP authentication successfully.

Radio Type

Indicates the type of radio installed in the device. For example:

- BG - Indicates a Summit 802.11g radio which supports 802.11b and 802.11g.
- ABG - Indicates a Summit 802.11a/g radio which supports 802.11a, 802.11b, and 802.11g.
- N - Indicates a Summit 802.11n radio which supports 802.11a, 802.11b, 802.11g, and 802.11n.

Reg. Domain

Indicates the regulatory domain(s) for which the radio is configured, including FCC, ETSI, TELEC, and KCC.

Note: See Channels for additional information on regulatory domains and DFS channels.

Auto Profile

Auto profile enables you to activate or deactivate automatic profile selection. Tap **List** and use the dialog box to select a created profile.

Note: Auto Profile is only available on Windows CE and Windows Mobile operating systems.

When a facility is active and the radio makes its first attempt to associate to an AP (after a device startup or resume), SCU tried each profile, in order, until the radio associates to an AP. That profile becomes the active profile and remains the active profile until one of the following occurs:

- The device is suspended and resumed, power-cycled, or restarted, which causes the automatic profile selection process to restart.
- The user turns off the automatic profile selection facility and manually selects a different profile on the SCU Main Window.

Note: The profile list should not include any profiles with an Ad Hoc Radio Mode setting.

There is a limit of 19 profiles in the Auto Profile list.

Auto Profile is not available for the MSD30AG and SSD30AG modules.

Driver

Indicates the current version of the device driver/

SCU

Indicates the SCU version currently running on the device. Displays only if space permits.

Import/Export

Displays only if the radio is programmed to allow import/export functions and if you are logged in as an administrator.

Tap Import/Export to do one of the following:

- Export global settings, all standard SCU profiles, and the special ThirdPartyConfig profile from the SCU area of a device's registry to a file that can be transferred to another device.
- Import global settings, all standard SCU profiles, and the special ThirdPartyConfig profile from a file (created using the Export facility) to the SCU area of a device's registry to enable SCU to use the information.

Note: When importing information, select Add to existing to merge new information with current registry information. Select Replace to overwrite the current registry information with the newly-imported information.

Profile Window

Profile settings are radio and security settings that are stored for each configuration profile. When a profile is selected as the active profile on the Main Window, the settings for that profile become active.

Note: When the ThirdPartyConfig profile is selected, a power cycle must be performed.

Figure 2 shows the SCU Profile windows for Windows CE and Windows XP operating systems.

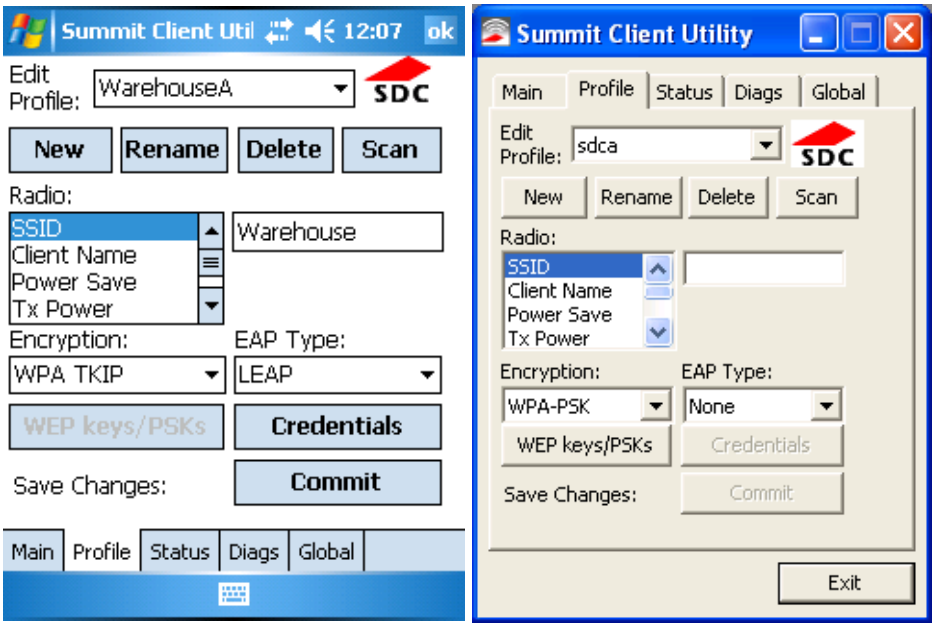


Figure 2: SCU Profile Window in Windows CE (left) and Windows XP (right)

From the Profile window, an administrator can:

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

Note: Profile changes are not saved to the profile until you tap Commit.

Note: If the Default profile is not modified, it does not specify an SSID, an EAP Type, or a data encryption method. As a result, if the Default is the active profile, then the radio associates only to an AP that broadcasts its SSID and requires no EAP type and no encryption.

The following describe the SCU Profile window properties and options:

Edit Profile

Use the drop-down menu to select the profile to be viewed or edited.

Profile Window Actions

You can perform the following actions from the Profile Window:

- New - Create a new profile with default settings. Assign a unique name (a string of up to 32 characters). Edit profile settings using other profile window selections.
- Rename - Change the profile name to one that is not assigned to another profile.
- Delete - Delete a non-active profile.

Note: You cannot delete an active profile.

- Scan - Tap to view a list of APs that are broadcasting SSIDs; select an SSID and create a profile for it.

Note: See "Using Scan to Create a Profile" for more information.

Using Scan to Create a Profile

When you tap **Scan** on the Profile window, SCU displays a list of APs that are broadcasting their SSIDs. Figure 3 below is an example of a Scan window.

Each row shows 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 tapping on the column headers. If the scan finds more than one AP with the SSID, the list displays the AP with the strongest RSSI and the least security. Every five seconds, the Scan window updates the RSSI value for each of the APs in the list. To scan for new APs and view an updated list, tap **Refresh**.

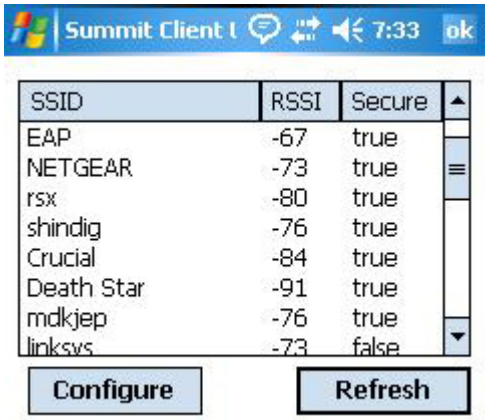


Figure 3: Scan Window

If you are authorized as an administrator in SCU, you can create a profile for any SSID in the list. To create a profile, double-tap the row for the SSID; or tap the row and then tap **Configure.**

If you tap **Yes** on the dialog box, then SCU creates a profile for that SSID, with the profile name being the name of the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already). If the AP is using WEP, then SCU opens a dialog box in which you can specify WEP keys. If the AP is using EAP, then SCU opens a dialog box in which you can specify login credentials for the EAP type (which SCU assumes is LEAP). After you enter information on a dialog box, you return to the SCU Profile window, where you can view and edit profile settings. If you make any changes, then you must tap Commit to save the changes.

Figure 4: Create a New Profile

Radio Settings

Select a radio attribute from the list on the left to view or edit its value or setting in the box on the right.

Note: The Summit Glossary of Technical Terms provides detailed information for the following radio setting terms located on the Profile Tab.

SSID	Service set identifier for the WLAN to which the radio connects. ▪ Value - A string of up to 32 characters ▪ Default - None
Client Name	The name assigned to the Summit radio and the client device that uses it. ▪ Value - A string of up to 32 characters ▪ Default - None
Power Save	Indicates the radio's current power save setting. Power save mode allows you to set the radio to its optimum power-consuming setting. ▪ Value: ▪ CAM - Constantly Awake Mode ▪ Maximum - Maximum power savings ▪ Fast - Fast Power save mode ▪ Default - Fast **Note:** When Wi-Fi power save is set to CAM, Bluetooth does not function properly. This issue only applies to Laird 40 series radios.

Bit Rate

Indicates the bit rate used by a radio when interacting with a WLAN 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 or 54/
- Maximum - Maximum defined for current regulatory domain
- Default - Auto

Note: If you select a specific bit rate, then the radio connects to an AP only if that AP has the specified SSID configured with the selected bit rate as the only required rate.

Note: This feature is not supported when using the SDC - MSD30AG and SDC - SSD30AG WLAN modules. When using the SDC - MSD30AG or SDC - SSD30AG modules, the Bit Rate option is unavailable. It defaults to Auto.

Radio Mode

Radio mode is a SCU Profile setting that indicates the use of 802.11a, 802.11g, 802.11b, and 802.11n frequencies and data rates when interacting with an access point, or the use of ad hoc mode to associate to a client radio instead of an access point. When SCU operates with a Summit 802.11g radio, an administrator can select from among the following radio mode values:

- 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 Subset - 1, 2, 5.5, 6, 11, 24, 36, and 54 Mbps. This should only be used with Cisco APs running IOS in autonomous mode (without controllers). For Cisco APs that are tied to controllers and for non-Cisco APs, Laird recommends BG rates full
- Ad Hoc – The radio uses ad hoc mode instead of infrastructure mode. In infrastructure mode, the radio associates to an AP. In ad hoc mode, the radio associates to another client radio that is in ad hoc mode and has the same SSID and, if configured, static WEP key
- CAM - Constantly Awake Mode
- Default - BG rates full

When SCU operates with a Summit 802.11a/g radio, an administrator can select from the following radio mode values:

- 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
- A rates only - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (same as G rates)
- ABG rates full - All A rates and all B and G rates, with A rates (the 802.11a radio) preferred
- BGA rates full - All B and G rates and all A rates with B and G rates (the 802.11g radio) preferred
- BG Subset - 1, 2, 5.5, 6, 11, 24, 36, and 54 Mbps. This should only be used with Cisco APs running IOS in autonomous mode (without controllers). For Cisco APs that are tied to controllers for non-Cisco APs, Laird recommends BG rates full
- Ad Hoc - When selected, the radio uses ad hoc mode instead of infrastructure mode. In infrastructure mode, the radio associates to an AP. In ad hoc mode, the radio associates to another client radio that is in ad hoc mode and has the same SSID and, if configured, static WEP key.
- Default - ABG rates full

Auth Type	Indicates the 802.11 authentication type used when associating to an access point. ▪ Value - Open, shared-key, or LEAP (Network-EAP) ▪ Default - Open **Note:** The Summit Client Utility refers to Network-EAP as LEAP.

Security

Values for the two primary security attributes, EAP type and encryption type, are displayed in separate drop-down lists with the current values highlighted.

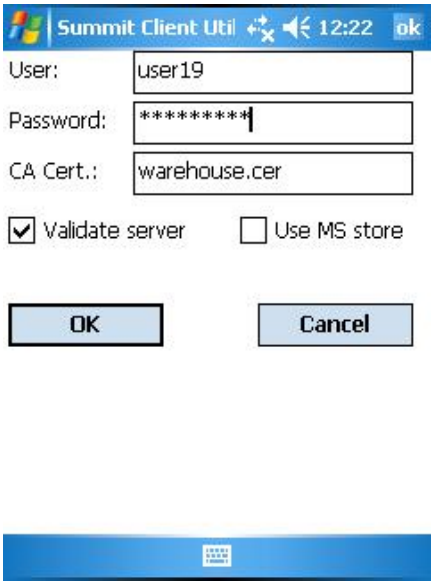
- Encryption - When you select an encryption type that requires the definition of WEP keys or a pre-shared key (PSK), the WEP keys/PSKs button becomes active. Tap WEP keys/PSKs to define WEP keys or a PSK.

Note: Laird Wi-Fi radios support two special access point settings:
- WPA Migration Mode
- WPA2 Mixed Mode

Note: When running Migration Mode (which is Static WEP and WPA-PSK), a client using PSK fails to obtain an IP address (and therefore can't pass traffic). The issue may arise if the user is running both Migration Mode and Mixed Mode (Static WEP/WPA-PSK/WPA2-PSK).

- EAP Type - When you select an EAP type, the Credentials button becomes active. Tap Credentials to define authentication credentials for the selected EAP type.

Entering Credentials for EAP Authentication



There are no default values for credentials. If the credentials are not specified in the profile then, when the radio tries to associate using that profile, Summit software displays a dialog box that prompts the user to enter the credentials. Summit software populates the dialog box with the username and password supplied for the previous EAP authentication.

Important notes on entering credentials for EAP authentication:

- If the credentials specified in the profile do not match those in the authentication database then, when that profile is used:
  - If the EAP type is EAP-FAST or EAP-TLS, authentication fails.
  - If the EAP type is LEAP, PEAP-MSCHARP, PEAP-GTC, or EAP-TTLS, then Summit software stores the valid credentials in the profile.
- When prompted with a dialog box, the user can enter valid credentials, enter invalid credentials, or cancel the operation:
  - If the user enters valid credentials and taps **OK**, the radio associates and authenticates.
  - If the user enters invalid credentials and taps **OK**, the radio associates but does not authenticate, and the user is re-prompted to enter credentials.
  - If the user taps **Cancel** or the user clears the credentials fields and taps OK, then the radio does 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 **Reconnect** on the Diags window
    - Modifies the profile and taps **Commit**
  - Alternatively, the user can select another profile as the active profile and then switch back to the profile for which EAP authentication was cancelled.
- If the password stored in the profile or provided in the dialog box has expired in the authentication database, then the authentication server may send an "Expired Password" (RFC 2759) message to the client. If the EAP type is PEAP-MSCHAP, PEAP-GTC, or EAP-TTLS, then the Summit software handles that message by displaying a dialog box that prompts the user to enter the expired password and a new password. Summit software then uses the entered information to respond to the RFC 2759 message. If EAP authentication succeeds and the expired password was saved in the profile, then Summit software updates the profile with the new password.
  - Any password provided for EAP authentication, whether in a profile or in an authentication dialog box, should not contain parentheses. Neither SCU or the dialog box flags a parenthesis as an invalid character, but the integrated supplicant treats parentheses as delimiters and interprets the characters between the left parenthesis and a right parenthesis as the "true" password.

Save Changes

To save changes for the selected profile, tap **Commit.**

Note: When you tap **Commit**, a registry flush occurs for only that profile key.

Status Window

The Status Window provides status information on the radio connection between the client device and the access point to which it is associated.

Figure 4 shows the SCU Status windows for Windows CE and Windows XP operating systems.

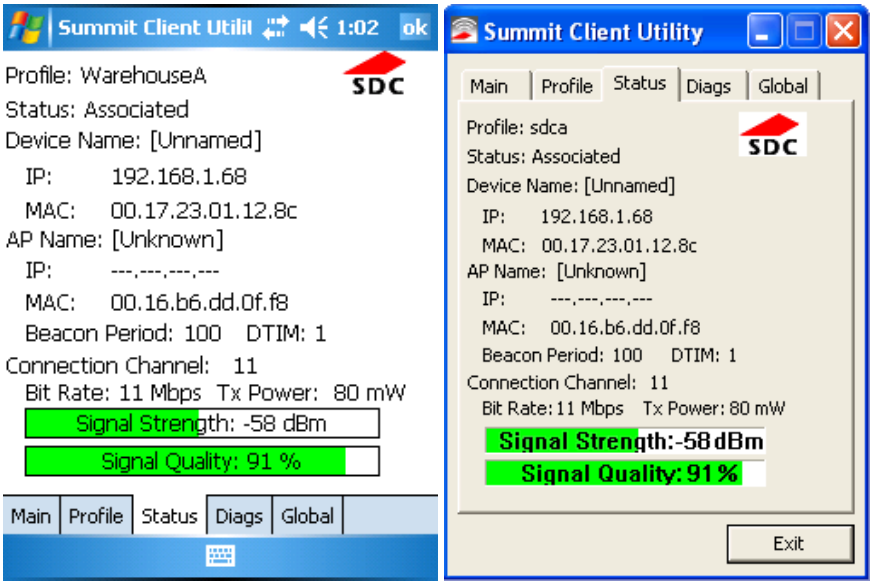


Figure 4: Status window

The following describe the SCU Status window properties and options:

- Profile
- Status
- Device Information
- AP Information
- Connection Information

Profile

Indicates the current active SCU profile.

Status

Indicates the current status of the radio.

Note: Status also displays on the Main tab window. See Main Window > Status for details on individual status options.

Device Information

Device information including the device name, IP address, and MAC address.

AP Information

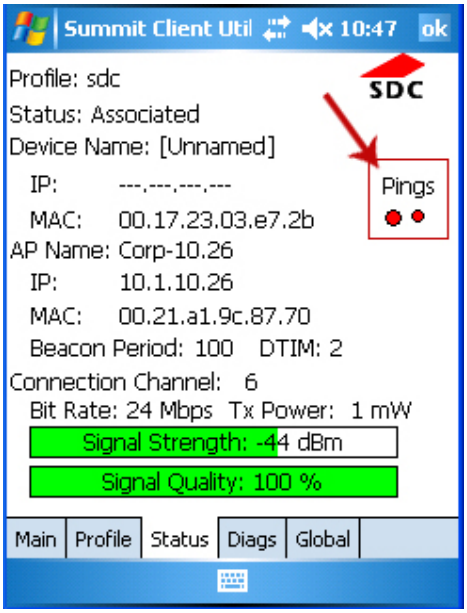
Access point information including the name of the access point to which the radio is associated, the IP address of the access point, and the MAC address of the access point. Also displayed in this section are the beacon period and DTIM.

Connection Information

Connection information including the channel the radio is using to connect to the access point along with the bit rate (in Mbps) and transmit power. This section also displays the signal strength (or RSSI) in dBm and quality.

Note: This value will be lower with a ThirdPartyConfig profile (under Windows Zero Config) that with a standard profile.

Note: When a ping initiated from the Diags window is active, the Status window displays a ping indicator consisting of two lights that flash green (for a successful ping) or red (for an unsuccessful ping).



Diags Window

The Diags window enables you to troubleshoot connection issues with SCU. Figure 5 shows the SCU Diags windows for Windows CE and Windows XP operating systems.

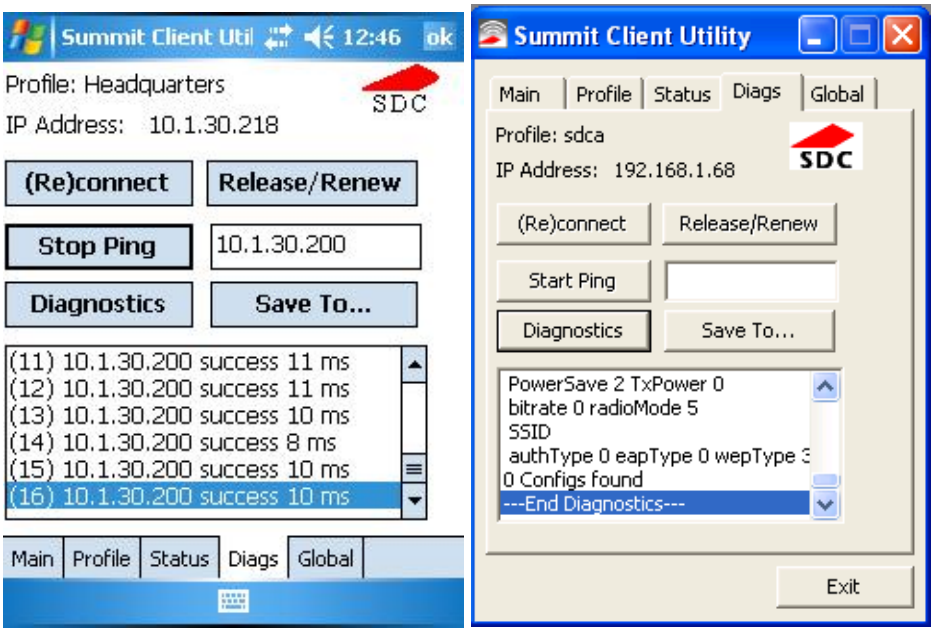


Figure 5: Diags window on Windows CE (left) and Windows XP (right)

The following describe the SCU Status window properties and options:

- (Re)connect
- Release/Renew
- Start Ping/Stop Ping
- Diagnostics
- Save To...

(Re)connect

Initiate a reconnect of the radio: Disable and enable the radio, apply (or reapply) the current profile, attempt to associate to the wireless LAN, and attempt to authenticate to the wireless LAN. SCU logs all activity in the output area at the bottom of the Diags window.

Release/Renew

Obtain a new IP address through DHCP release/renew. SCU logs all activity in the output area at the bottom of the Diags window.

Start Ping/Stop 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 changes to Stop Ping. Pings continue until you tap Stop Ping, move to a different SCU window (other than Diags or Status), exit SCU, or remove the radio.

Note: If your device has both a Laird Wi-Fi radio and another network adapter active, then pings may go out over the non-Laird network adapter.

Note: The access point's IP address is the default for a ping although any valid IP address can be manually entered.

Diagnostics

Attempt to reconnect to an access point and provide a more thorough dump of data than is obtained with (Re)connect. The dump includes radio state, profile settings, global settings, and a BSSID list of access points in the area.

Save To...

Indicate where you want to save the diagnostics file. Tap **Save To...** to open the *Save As* window. From here, you can change the SDC diagnostics file name, the folder in which the SCU saves the file, the format in which the file is saved (the file type), and the location of the saved file (Main memory or System).

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.

Figure 6 shows the SCU global windows for Windows CE and Windows XP operating systems.

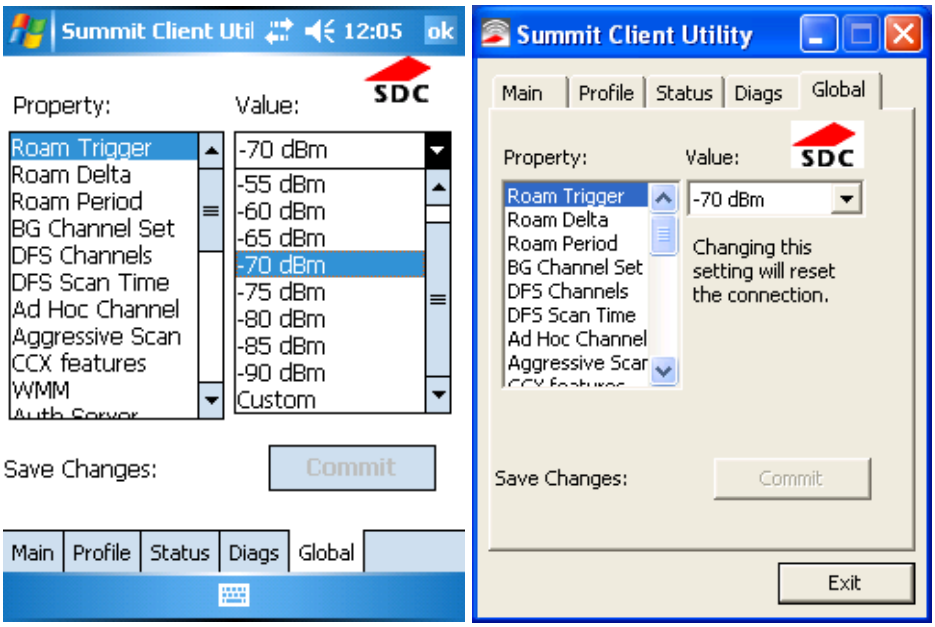


Figure 6: Global Window in Windows CE (left) and Windows XP (right)

Note: When you tap **Commit**, a registry flush occurs of all global settings.

Roam Trigger

Roam trigger indicates the signal strength (RSSI) (in dBm) at which the radio scans for an access point with a better signal strength. When scanning for a different access point, the radio looks for one with a RSSI at the indicated roam delta dBm level or stronger.

- Values: -50, -55, -60, -65, -70, -75, -80, -85, -90, or Custom (See "Custom Global Settings" for more information)
- Default: -70

Note: When reporting RSSI: The 10, 15, 20, 25, and 40 series Laird Wi-Fi radios use a Broadcom chip set. The radios return the absolute RSSI (a full signal) regardless of ambient noise. In high noise situations, in may be necessary to reduce the roam trigger level to compensate for this. The 30 series Laird Wi-Fi radios use a Qualcomm/Atheros chip set. These radios return the relative RSSI (a useable signal) above ambient noise. In high noise situations, it may be necessary to increase the roam trigger level to compensate for this (and add 'stickiness').

Roam Delta

Roam delta indicates the signal strength (RSSI) level (in dBm) that the radio looks for in a different access point (after the roam trigger is met) before it attempts to roam to the new access point.

- Values: 5, 10, 15, 20, 25, 30, 35, or Custom (See "Custom Global Settings" for more information)
- Default: 10

Roam Period

Roam period indicates the amount of time a radio collects RSSI scan data (after association or a raom scan) before it considers roaming to a different access point.

- Values: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, or Custom (See "Custom Global Settings" for more information)
- Default: 10

BG Channel Set

Indicates the 2.4 GHz channels that the radio scans when contemplating a roam to determine what access points are available. BG channel set options include:

- Full - The radio scans all 2.4 GHz channels
- 1, 6, 11 - The radio scans the three most commonly used 2.4 GHz channels
- 1, 7, 13 - The radio scans for ETSI and TELEC certified radios only
- Custom - 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 **Custom** and tap **Commit**, then SCU reverts to the value that it displayed before you selected Custom.

- Default: Full

DFS Channels

Indicates support (or lack of support) for 5 GHz (802.11a) channels where dynamic frequency selection (DFS) is required. This setting is supported in v2.0 and later.

Values:

- On - Turns on support for 5 GHz channels where DFS is required
- Off - Turns off support for 5 GHz channels where DFS is required
- Optimized - When set to Optimized and scanning for the first time, the radio scans all active channels and all available DFS channels. From this scan, the radio creates and maintains a list of up to three DFS channels where beacons were detected. During subsequent scans, the radio still scans all active channels but only scans the DFS channels listed from the first scan (where beacons were detected).
- Default: Off

Note: When the radio loses or resets the connection, the radio returns to scanning all available DFS channels as it did when scanning for the first time after being set to Optimized. From this scan, the radio again creates a list of DFS channels where beacons were detected.

Note: The Optimized setting is not supported in the MSD30AG and SSD30AG radios. If DFS Channels is set to Optimized directly in the registry, this setting will function as On (versus Optimized).

DFS Scan Time

Because passive scanning consumes a longer period of time, this feature enables you to determine the dwell (listen) time when passively scanning on a DFS channel.

- Value: A number between 20 - 500 milliseconds (ms)
- Default: 120 ms

When decreasing the scan time (to a value lower than the default) for DFS channels, corresponding changes in the infrastructure's beacon period are recommended. For optimal performance and reliability, Laird recommends a dwell time that is 1.5 times that of the beacon period. For example, if the DFS scan time is set to 30 milliseconds, the beacon period should be adjusted to 20 milliseconds.

If you adjust this parameter directly in the registry, the setting value will return to the default (120 ms) if configured to a number outside of the 20 - 500 ms range.

Ad Hoc Channel

Ad Hoc Channel is a SCU Global setting that indicates the channel to be used for an ad hoc connection if the active profile has a Radio Mode value of Ad Hoc.

Values:

- One of the 2.4 GHz channels (1 - 14)
- One of the UNII - 1 channels (36, 40, 44, 48)
- Default: 1

Note: If you select a channel that is not supported by your radio, then SCU uses the default channel setting (1) for this setting.

Aggressive Scan

When this setting is On and the current connection to an access point becomes tenuous, the radio scans for available access points more aggressively. Aggressive scanning complements and works in conjunction with the standard scanning that is configured through the Raom Trigger, Roam Delta, and Roam Period settings. Laird recommends that the Aggressive Scan global setting be On unless there is significant co-channel interference because of overlapping coverage from access points that are on the same channel.

- Value: On or Off
- Default: On

CCX Features

CCX features is an SCU Global setting that enables the use of the Cisco information element (IE) and CCX version number to authorize support for CCX features.

Values:

- Full - Use Cisco IE and CCX version number and enable support for all CCX features
- Optimized - Use Cisco IE and CCX version number and enable support for all CCX features except AP-assisted roaming, AP-specified maximum transmit power, and radio management
- Off - Do not use Cisco IE and CCX version number
- Default: Optimized

Note: For Summit 30AG (SDC - MSD30AG and SDC - SSD30AG) radio modules, this parameter is disabled.

WMM

WMM (Wi-Fi Multimedia) extensions for WLANs allow the prioritization of voice traffic.

WMM is an SCU Global setting that enables or disables the use of WMM extensions.

- Value: On or Off
- Default: Off

Note: If you change the WMM global setting in SCU, you must do a power cycle or suspend/resume on the device to cause the change to take effect.

Note: For ABGN radio modules, this parameter is disabled.

Auth Server

Auth Server is an SCU Global setting that indicates the type of authentication server being used for EAP.

Values:

- Type 1 - Cisco Secure ACS or another server that uses PEAPv1 for PEAP with EAP - MSCHAPV2 (PEAP - MSCHAP)

  - Allows the authenticated or anonymous PAC provisioning
  - Limits the inner methods to EAP_FAST, PEAP_MSCHAPV2, and PEAP_GTC
- Type 2 - A different authentication server, such as Juniper Networks Steel Belted RADIUS, that uses PEAPv0 for PEAP_MSCHAP
  - Only allows authenticated PAC provisioning
- Default: Type 1

TTLS Inner Method

TTLS Inner Method is an SCU Global setting that indicates the authentication method that is used within the secure tunnel created by EAP - TTLS.

Values:

- Auto-EAP - Any available EAP method
- MSCHAP
- MSCHAPV2
- PAP
- EAP-MSCHAPV2
- Default: Auto-EAP

PMK Caching

PMK (Pairwise Master Key) Caching is an SCU Global setting that indicates the type of PMK caching to use (Standard or OPMK) with a WPA2 encryption type.

- Value: Standard or OPMK
- Default: Standard

Note: When switching from Standard to OPMK, you must initiate a suspend resume of the device. Only tapping Commit does not cause the change to take effect.

Tx Diversity

Antenna diversity refers to the use of multiple antennas to increase the odds that a functional signal is received.

Tx (Transmit) Diversity is an SCU Global setting that indicates how to handle antenna diversity when transmitting data to an access point.

Values:

- Main only - Indicates use of the main antenna only
- Aux only - Indicates use of the auxiliary antenna only
- On - Indicates the use of diversity (both antennas)
- Default: On

Note: Laird does not support the AUX antenna as a single-antenna solution.

Note: For 30AG (MSD30AG and SSD30AG) radio modules, this parameter is disabled.

Rx Diversity

Antenna Diversity refers to the use of multiple antennas to increase the odds that a functional signal is received.

Rx (Receive) Diversity is an SCU Global setting that indicates how to handle antenna diversity when receiving data from an access point.

Values:

- On-Start on Main - Indicates use of the main antenna upon startup
- On-Start on Aux - Indicates use of the auxiliary antenna upon startup
- Main only - Indicates use of the main antenna only
- Aux only - Indicates use of the auxiliary antenna only
- Default: On-Start on Main

Note: Laird does not support the AUX antenna as a single-antenna solution.

Note: For 30AG (MSD30AG and SSD30AG) radio modules, this parameter is disabled.

LED

LED is an SCU Global setting that indicates whether or not an LED is used.

- Value: On or Off
- Default: Off

LED On = Connected to the network

LED Off = Not connected to the network

Note: No flashing functionalist is supported.

SCU Global Settings

The following SCU global settings, which apply to SCU and other Laird applications, can be changed in SCU:

- Tray Icon
- Hide Passwords
- Admin Password
- Auth Timeout s
- Certs Path
- Ping Payload
- Ping Timeout ms
- Ping Delay ms
- Custom Global Settings

Tray Icon

Tray Icon is an SCU Global setting that allows you to enable or disable the System Tray icon.

The tray icon provides a visual status for the device's Laird Wi-Fi radio and it enables the user to launch SCU. This service is available only for Windows CE and Windows Mobile.

- Value: On or Off
- Default: On

Hide Passwords

Hide Passwords is an SCU Global setting that indicates whether or not passwords are masked. If this setting is turned on, SCU (along with EAP authentication dialog boxes) masks passwords, WEP keys, and other sensitive information.

- Value: On or Off
- Default: Off

Admin Password

Admin Password is an SCU Global setting that indicates the password that must be specified when the Admin Login button is tapped.

- Value: A string of up to 64 characters
- Default: SUMMIT (case sensitive)

Auth Timeout s

Auth Timeout is an SCU Global setting that specifies the number of seconds (from 3 to 60) that Laird software waits 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 is re-prompted to enter authentication credentials.

- Value: An integer from 3 to 60
- Default: 8

Certs Path

Certs Path is an SCU Global setting that indicates the directory location for certification(s) for EAP authentication and PAC files. A valid directory path can include up to 64 characters and the default depends on the type of device.

- Value: A valid directory path of up to 64 characters
- Default: Depends on the device

Ping Payload

Ping Payload is an SCU Global setting that indicates the amount of data (in bytes) that is transmitted on ping.

- Values: 32, 64, 128, 256, 512, 1024
- Default: 32

Ping Timeout ms

Ping Timeout is an SCU Global setting that indicates the amount of time (in milliseconds or ms) that passes without a response before the ping request is considered a failure.

- Value: An integer from 1 to 30,000
- Default: 5,000 ms

Ping Delay ms

Ping Delay is an SCU Global setting that indicates the amount of time (in milliseconds or ms) between successive ping requests.

- Value: An integer from 0 to 7,200,000
- Default: 1,000 ms

Custom Global Settings

If SCU displays a value of "Custom" for 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 not real effect. If SCU displays a value other than Custom and you select the value of Custom and tap **Commit**, then SCU reverts to the value that it displayed before you selected Custom.

Note: There is a range of accepted value for each of these global settings. Any value placed in the registry outside of the following acceptable ranges will reset the value back to its default:

- Roam Trigger acceptable range: 50 to 90
- Roam Delta acceptable range: 1 to 35
- Roam Period acceptable range: 1 to 60
- BG Channel acceptable valid inputs: 0001 to FFFF

USING THE SUMMIT SYSTEM TRAY ICON (WINDOWS CE AND MOBILE ONLY)

On Windows CE or Windows Mobile, Laird Wi-Fi software includes a service that displays an icon in the Windows System Tray. This icon provides a visual status for the device's radio and it enables the use to launch SCU. This service is available only for Windows CE and Windows Mobile.

The software for the service is installed with other Laird Wi-Fi software in a .cab file. The service is active only when all of the following are true:

- When the service 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

When the service is active, it queries the driver every three seconds for the status of the connection for the active profile and displays one of the following icons:

	The radio is not associated/authenticated to an access point.
	The signal strength (RSSI) for the current access point (to which the radio is associated) is -90 dBm or weaker, which means that a Summit 802.11b/g radio will operate at 802.11b data rates only.
	The RSSI for the current access point is stronger than -90 dBm but not stronger than -70 dBm, which means that a Summit radio will operate at 802.11g or 802.11a data rates that are less than 54 Mbps.
	The RSSI for the current access point is stronger than -70 dBm but not stronger than -50 dBm, which means that a Summit radio should operate consistently at 54 Mbps
	The RSSI for the current access point is stronger than -50 dBm

Tapping the icon launches the SCU. On most CE devices, the System Tray icon is not visible while SCU is running, although the service remains active.

Note: 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.

REGISTRY SETTINGS

Customized Roaming

The roaming behavior of a Laird WI-Fi radio module can be adjusted through two collections of configuration settings:

- Global settings: Can be altered in SCU or through the SDK
- Registry settings: The following registry settings can be used to "tune" roaming.

Parameter	Description	Value	Default
Probe Delay	Number of seconds between scans when the radio is not associated. Lower numbers result in faster reconnects but also more power draw when not associated. Not applicable to WZC.	Integer in the range of 2 - 60	10
Average Window	The number of RSSI samples that the radio should use to calculate moving average RSSI.	Integer in the range of 2 - 8	8

Probe Delay

Probe delay affects two things:

- How quickly an association occurs when in a Not Associated state
- Battery life

The following is an example of a situation where ***quick*** is more important:

The user is driving a forklift quickly through a warehouse and hits a dead zone (no coverage). The radio on the forklift enters a Not Associated state. Upon entering another coverage area, the user wants the radio to re-associate as quickly as possible given the speed of the vehicle. If the Probe Delay is set to a low value of 2, the radio attempts to re-associate every two seconds. If the Probe Delay is set to 60, the radio attempts to re-associate every 60 seconds. In this situation, the Probe Delay should be set to a low number to ensure that the vehicle's radio re-associates as quickly as possible when it enters AP range.

Because the device is mounted on a forklift and typically receives its power from the vehicle's battery, the battery life of the device is not an issue in this situation.

The following is an example of a situation where ***battery life*** is more important:

The user is driving a vehicle that occasionally travels outdoors to an area that is outside of the 802.11 coverage. If the device is running on battery power and is out of coverage for extended periods with little or no possibility of associating to an AP, the Probe Delay value should be set to a high number. If the radio attempts to re-associate every two seconds, the batter power will run down more quickly than if the Probe Delay is set to sixty seconds. In this situation, battery life is more of an issue than a quick association time.

The ideal Probe Delay value is probably somewhere between 2 seconds and 60 seconds, based on whether or not it is running on battery and whether or not the device is expected to go out of coverage for extended periods or brief periods of time.

RSSI Samples

RSSI is the relative received signal strength in a wireless environment. The RSSI value is an eight sample moving average which includes data and beacons on the AP's base beacon transmission method (CCK or OFDM).

The Laird WI-Fi radio decides when it should begin looking for a new AP when it crosses the Roam Trigger (set from the Global tab on the SCU); the Roam Trigger is based on the RSSI. In theory, the radio is less likely to scan for a new AP based on missed beacons if there are a greater number of values in the average. The reverse occurs (the radio is more likely to scan because of missed beacons or an occasional poor RSSI reading) if there are fewer numbers in the average. In practice, the default value of 8 provides a smoother transition across the Roam Trigger but takes longer to reach than with the shorter values. Low values may result in quicker roams (depending on what the radio sees when it scans), but may also result in unnecessary roams in noisier environments since you are more likely to cross the threshold more quickly if you are only average two values together to find the average RSSI.

Power Management

V2.01.17 introduced a power management scheme that enables Laird WI-Fi software to pass Windows Mobile 6.1 Logo Test Kit (LTK) testing. This scheme may cause issues on some devices that run CE.NET 5.0.

To revert to the scheme that was supported in releases prior to V2.01.17, do the following:

- Create a DWORD value called noWDM in the Global Config area of the registry.
- Set a value to 3.
- Perform a power cycle to ensure that the driver recognizes the registry entry.

To remove all power management capabilities for troubleshooting purposes, set the noWDM key to a value of 1 and then perform a power cycle.

Typically, one of these Power Management settings will work property for a given device. Setting the value at 3 informs the operating system that our driver does not support sleep modes and that the driver should force an unloading/reloading on a suspend/resume.

If this value is set to 0, Power OIDs (object identifiers) are sent upon suspend/resume. Some devices have issues with these OIDs. Check with your network administrator for the correct setting for your device.

Handling Interference

The Interference Mode registry setting introduced in V2.00.38 affects how the radio responds to different types of interference:

- Off (0): Do not adjust for interference
- Non-WLAN (1): Reduce the noise floor threshold for transmits so that the radio transmits even when there is non-WLAN noise. Note that this setting may increase the impact of Laird WI-Fi radio transmissions on other WLAN devices in the vicinity.
- WLAN (2): Tighten the frequency range for the channel to reduce the effects of interference from adjacent channels. Note that this setting may cause a significant reduction in the Laird WI-Fi radio's received sensitivity.
- Off (3): Do not adjust for interference (same as 0). This is the default setting.

Interference Mode

This setting can be used for both environmental noise and noise inside of a device (as a result of antenna routing or radio proximity to 2.4 GHz or 5 GHz emitters). With a value setting of 1 (which lowers its noise floor when doing clear channel assessments), the device is less sensitive to noise created by non-802.11 devices. If will not be deterred from transmitting because of noise that might otherwise indicate the channel is in use.

Note: This setting allows the device to better compete with other devices such as microwave ovens, but it may affect the ability of weaker 802.11 devices to communicate.

A value setting of 2 narrows the frequency range and is useful if you have noise from an adjacent channel. This provides the radio with an increased ability to communicate despite WLAN activity on an adjacent channel but may cause lower receiver sensitivity (which means lower data rates and/or a decreased coverage area).

The recommendation is to use the default setting (Off [3]) and remove or reduce environmental noise. If this is not possible, you can experiment with the Interference Mode settings as necessary, depending on whether or not the noise is from an 802.11 source.