# LAIRD WIRELESS SOFTWARE

## Usage Notes v1.0

## INTRODUCTION

Summit brand Wi-Fi products from Laird Technologies operate on the following operating systems:

- Windows Embedded CE 5.0, 6.0, 6.0 R2, or 6.0 R3
- Windows Mobile 2003, 5.0, 6.0, 6.1, or 6.5
- Windows XP or Embedded XP SP2 (or higher)
- Windows Embedded 7.0

These usage notes are related to Laird's 10, 15, 20, and 30 series Wi-Fi radios.

The following are software usage notes:

- **Windows Embedded CE 4.2:** Beginning with software release version 3.03.xxx, Windows Embedded CE 4.2 is no longer supported. Software version 3.2.9 is the final software release that supports Windows Embedded CE 4.2.
- **Summit SDK versions:** Applications compiled with v2.1 and v2.2 Summit SDKs continue to function with v2.3 drivers and files. However, due to changes for our new supplicant and new radios, we recommend that you recompile with a v2.3 SDK for better performance and support.
  If you plan to use 30AG or 15N radios in your application, you must upgrade your SDK to v2.3.

**Note:** For additional information regarding the SDK, refer to the Summit Developer Kit FAQ or the Summit Developer Kit Programmer's Guide available from the Laird Technologies website, here.

## REGISTRY SETTINGS

The following are Registry Setting usage notes:

- **Storing Summit brand software files in a custom location:** Refer to Installing Summit Software to Custom Locations for detailed information.
- **Coexistence with an intermediate driver:** Summit highly discourages the use of intermediate drivers because they can interfere with how SCU and the integrated Devicescape supplicant interact with the Summit device driver.
  **Note:** Both SCU and the supplicant communicate with the driver by opening the device directly.
  If an intermediate driver is installed on the device that blocks direct access to the device, you must change the setting of a registry key (*HKLM\Software\Devicescape\Supplicant\Interface\iface*) from SDCCF10G1 to the name assigned to the device by the intermediate driver. Even if you make this registry key change, Summit cannot guarantee full compatibility due to the nature of intermediate drivers.
- **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:** This may increase the impact of Summit 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:** This setting may cause a significant reduction in the Summit radio's receiver sensitivity.

  - Off (3): Do not adjust for interference (same as 0). - Default setting.

- **No prompting if profile credentials are bad:** The *noPromptForCreds* registry setting (introduced in V2.00.38) ensures that, if authentication using the crednetials in the active profile fails, the user is not prompted to enter valid credentials. Values are:
  - Off (0): Prompt the user if authentication using credentials in profile fails - Default setting
  - On (1): Do not prompt the user
- **Including profiles with .cab file:** Summit configuration profiles are stored in the registry. You can use a single .cab file to install Summit software and profiles.
  - V2.00.38 introduces changes to the format of profiles in the registry. With V2.00.38, if you want to install Summit profiles from a .cab file, you must set the following registry key to a DWORD value of 1: **HKLM\Comm\SDCCF10G1\Parms\InstallKey**
  - The use of this registry key informs Summit software to load profiles from the .cab file and ensure that the profiles have the proper formate in the registry.
- **Controlling Import/Export button:** SMU can establish a registry setting that causes a user logged into SCU as an administrator to see an Import/Export button on the SCU Main window. By tapping that button, the user views a dialog box which allows import or export of global settings, all standard SCU profiles, and the special ThirdPartyConfig profile. For details, see the SMU Guide.
  - If SMU does not establish the registry setting, then you can establish it manually. To cause the Import/Export button to appear, set the adminFiles key to 1 in the Global Config area: **HKEY_LOCAL_MACHINE\Comm\SDCCF10G1\Parms\Configs\GlobalConfig**
  - The next time the SCU is opened, the Import/Export button appears on the Main tab. To cause the button to disappear, repeat the above process and set the **adminFiles** key to 0.
- **Default profile setting:** To have SCU and SDK use your custom values when creating new profiles, enter the new defaults in the registry. Add an **HKLM\Comm\SDCCF10G1\Parms\Configs\DefaultConfigSettings** key. Under this key, you can add any of the profile keys.
  - To change the default PowerSave mode when users create new profiles in SCU add **PowerSave** (DWORD) with a value of 0 for CAM, 1 for Maximum, 2 for Fast. You can determine possible values by looking at the SDK documentation. Instead of directly editing the registry, you can also call the *SetDefaultConfigValues* in the SDK to write these registry keys.
- **MAC address spoofing:** MAC address spoofing allows you to change the MAC address of the client. In the global config area of the registry--*HKLM\Comm\SDCCF10G1\Parms\Configs\GlobalConfig* or *HKLM\Comm\SDCSD10G1\Parms\Configs\GlobalConfig*--spoof the MAC address by setting one or two keys:
  - **spoofOUI** - A DWORD that specifies the OUI of the MAC address (the first of three bytes).
  - **spoofUnit** - A DWORD that specifies the rest of the MAC address (the last three bytes).

If you do not include both of the keys, then only the designated part of the MAC address is changed.

## Cisco Wireless LAN Controllers

The following are usage notes for the use of Summit radios with a Cisco WLAN infrastructure that uses controllers:

- CCKM: A Cisco controller-based WLAN infrastructure supports Cisco Compatible Extensions (CCX) features only with clients that are certified for CCX Version 4 (V4). Those CCX features include CCKM, a Cisco-defined key management protocol for fast 802.1X reauthentication.

With Summit software V2.00.38 and above, Summit radios are certified for CCX V4 for ASDs. As a result, if you upgrade devices to V2.00.38 or above, you can use CCKM or any other CCX feature with a Cisco controller-based WLAN infrastructure or a Cisco autonomous (non-controller) WLAN infrastructure.

- Radio Mode: The BG subset (formerly *BG optimized*) value for the Radio Mode setting in a profile is optimized for Cisco APs running certain older versions of IOS in autonomous mode (without controllers). This Radio Mode value is not optimized for and should not be used with Cisco APs that are tied to controllers or in autonomous mode with a current version of IOS.
  Beginning with V2.00.38, the default value for Radio Mode is *BG rates full*.

## Security Configuration Elements

The following are Security Configuration Elements usage notes:

- **CCKM with WPA2:** To use CCKM with WPA2 AES, ensure that your Cisco APs run a version of IOS that supports CCKM with WPA2 AES. For 16 MB platforms such as the AP1100 and AP1230, the minimum version of IOS is 12.3.8-JEC2. For 32 MB platforms such as the AP1130, AP1240, or AP1250, the minimum IOS version is 12.4.10b-JDA.
- **CCKM/AES support:** CCKM/AES is supported in the SDC-MSD30AG and the SDC-SSD30AG radios beginning with version 3.03.09.
- **WPA handshake timeout:** When Summit radios use WPA or WPA2 to connect to Cisco APs that run IOS, Summit recommends that you configure the WPA handshake timeout on the APs to a value of 1,000 milliseconds. To configure the timeout, Cisco offers the following command line interface (CLI) command: *dot11 wpa handshake timeout*. This command enables you to adjust the amount of time that the AP waits before timing out WPA key packet transmission. The syntax of the command is:
  dot11 wpa handshake timeout *time*
  where time specifies the timeout time in milliseconds. The valid range for the timeout value is 100 ms to 2,000 ms. The default is 100 ms.
  For details on the CLI command, see Cisco documentation such as the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.3(8)JA.
- **EAP authentication passwords:** 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.
- **Switching to EAP-FAST:** If you use SCU to configure a profile for PEAP or EAP-TLS with validation of the server, and then use SCU to switch the EAP type to EAP-FAST without changing the credentials, then EAP-FAST automatic provisioning fails because the "leftover" certificate information in the profile is treated as a manual PAC filename. Whenever you change the EAP type in a profile, be sure to configure the credentials for the new EAP type.
- **CKIP:** If the active profile has an Encryption setting of CKIP or CKIP EAP, then the Summit radio associates or roams 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**

## Notes on Power Management

The following are Power Management usage notes:

- **Minimizing power draw of disabled radio:** When you use SCU to disable a Summit radio, the Summit driver a software disable of the radio and the disabled radio continues to draw some power. To fully disable the radio, you must remove power from the radio slot. Beginning with V2.02.16, Summit software on Windows Embedded CE and Windows Mobile enables you to run a custom function when the radio is disabled and a different custom function when the radio is enabled.
  - Implement the custom disable function in the *sdcWLANoff.exe* file stored in the *\Windows* directory. In this application, you can remove power to the slot or do whatever is necessary before a radio disable.
  - Implement the custom enable function to the *sdcWLANon.exe* file stored in the *\Windows* directory. In this application, you can send power to the slot or do whatever is necessary for a radio enable.
  - When it is about to disable the radio SCU first tries to run the *sdcWLANoff.exe* file in *\Windows.* If it cannot run that file successfully, then SCU calls the usual radio disable SDK function to disable the radio.
  - When it is about to enable the radio, SCU first tries to run the *sdcWLANon.exe* file in *\Windows.* If it cannot run that file successfully, then SCU calls the usual radio to enable SDK function to enable the radio. If you don't provide custom functions for radio disable and radio enable, then these operations proceed as normal.
  - **Return values from sdcwlanon or sdcwlanoff:** Summit brand software does not check return values from *sdcwlanon* or *sdcwlanoff.* If SCU is able to CreateProcess successfully, then we don't check any return values and do nothing else. If the CreateProcess fails (because File Not Found or another reason), SCU performs it's default behavior.

  **Note:** We recommend that if your sdcWLANon/off encounters an error, perform the default behavior: call our SDK's RadioDisable/RadioEnable and sleep for a minimum of 1500 ms.

- **Conserving power while not associated:** When it is not associated to an AP, a Summit brand radio periodically scans for an AP to which it can associate. To conserve device battery life, you can use the Probe Delay registry setting to lengthen the period of time between scans. Power Save Polling (PSP) can be used only while the radio is associated to an AP.
- **Long beacon periods or DTIM intervals:** If a Summit brand radio that is using a Fast or Maximum power save setting is associated to an AP with a beacon period or DTIM interval that is greater than one second, then the following things may occur:
  - The moving average RSSI value, which the radio compares to the Roam may be artificially low, causing the radio to do excessive scanning for a "better" AP.
  - If the Aggressive Scanning global setting is on, then the radio may do more aggressive scanning than it should.

## Usage Notes for the SDC-PE15N and 40-series Radios

The following usage notes apply specifically to the SDC-PE15N and 40-series radios:

- **WMM option:** On the Global tab of the SCU, the WMM option is grayed out and always set to be "enabled". This setting is required in order to properly operate with 802.11n rates but does not affect the radio's operation when using non-802.11n rates.
- **802.11n data rates:** On the Profile tab of the SCU, the Radio Mode should be set to ABG Full in order to take advantage of available 802.11n data rates.
- **802.11n bit rates:** On the Profile tab of the SCU, the Bit Rate should be set to Auto in order to be able to operate at 802.11n rates.

- **Profile encryption configuration:** A profile must be configured for no encryption or WPA2/AES in order for N rates to be used. The 802.11n standard does not permit N rates to be used with WEP or WPA/TKIP.
- **SDC-SSD40L and A band support:** SDC-SSD40L does not support A. Radio mode is BG full.

The following usage note applies specifically to the SDC-PE15N radio:

- **Maximum PSP:** When SCU Power Save is set to Maximum, the PE15N radio occasionally experiences intermittent communication.

## OTHER USAGE NOTES

The following are miscellaneous usage notes:

- **N-enabled Motorola AP setting change:** Motorola has determined that some legacy clients do not receive frames transmitted by its N-enabled APs when using the Dynamic Chain Selection setting. For A/B/G radios attempting to connect to an N-enabled Motorola AP (such as the 7131AP), Dynamic Chain Selection must first be turned off. Dynamic Chain Selection is enabled by default and must be disabled for our legacy clients to correctly function.
- **Antenna settings or AG radio:** Default values for ths global settings of Rx Diversity and Tx Diversity are the same for an AG radio as they are for a G radio, namely:
  - Rx Diversity: On-Start on Main
  - Tx Diversity: On

For an AG radio, these default settings assume that there are four antennas: two for 2.4 GHz (802.11b and 802.11g) and two for 5 GHz (802.11a). If your device uses an AG radio with two antennas, one for 2.4 GHz and one for 5 GHz, then you must change the Rx Diversity value to *Main Only* and the Tx Diversity value to *Main Only.*

- **SCU Scan and WEP vs. WEP EAP:** When you tap **Scan** on the Profile window, SCU opens a window that lists APs that are broadcasting their SSIDs. If you are authorized as an administrator in SCU and you double-click the row for an SSID or tap the row and tap **Configure,** then SCU creates a profile for that SSID. When the AP is using WEP, SCU cannot determine if the AP is using static WEP keys or dynamic WEP keys derived through the EAP authentication (WEP EAP). As a result, SCU opens a dialog box in which you can specify static WEP keys. If the AP is using WEP EAP, then you should close the static WEP dialog box and configure the appropriate EAP type.
- **Use of (Re)connect button:** After you tap **(Re)connect** on the SCU Diags window, wait for the operation to complete before taking another action on SCU or performing a suspend/resume on the device. If you perform another SCU action or a suspend/resume before the (re)connect operation completes, you may cause the Summit supplicant to fail with an exception error.
- **Log for Diagnostics output:** When you tap **Diagnostics** on the Diags window, SCU displays the output in the command output box on the window. In addition, SCU logs the output to a file named *_sdc_diag.txt* in the Windows directory. Because a text file can be viewed using a number of different editors, Laird Technologies has no plans to enhance the Diags window command output box with items such as a horizontal scroll bar.
- **Auto Profile list:** The list of profiles for the automatic profile selection facility should not contain any profiles with an Ad Hoc radio mode. If an ad hoc profile is included in the list then, when that profile is selected automatically, an ad hoc connection is not established and the profile is skipped.
- **Dual Ethernet Issue:** When using a Summit brand radio in a docking station with an Ethernet connection, if the Ethernet is active, the WLAN connection cannot function. To resolve this issue, use Windows Wireless Zero Configuration (WZC) to establish a WLAN connection.
- **Manage Passwords in SCU:** By default, SCU does not mask passwords or other sensitive data items such as WEP keys and pre-shared keys. To mask all sensitive data items in SCU, log in as Administrator, go to the Global tab, select **Hide Passwords** from the Property menu, select **On** from the Value drop-down menu, and

click **Commit.** An alternative is to edit the registry keys directly. Use the *displayPWDS* registry setting in the GlobalConfig area. The value of *displayPWDS* can be 0-3:

- **0:** Mask all passwords; leave option in the GUI to change it.
- **1:** Passwords are unmasked; leave option in the GUI to change it.
- **2:** Mask all passwords; GUI doesn't have the option to change it.
- **3:** Passwords are unmasked; GUI doesn't have the option to change it.

Each time SCU loads, the *displayPWDS* registry key in the global area (**HKLM\Comm\SDCCF10G1\Params\Config\GlobalConfig**) is checked. If the value is 2 or 3, the Hide Passwords setting is removed from SCU. In SCU, the user can only set 0 or 1. To remove the option (by setting the value to 2 or 3), it must be manually changed in the registry.

This password-masking setting affects the admin password, WEP keys, PSKs, and EAP credential passwords.

- **Setting the BG Channel Set to "Custom" in SCU:** If you set the BG Channel Set global setting to a value of Custom in SCU, then you must define a channel map in the global settings portion of the registry:
  **Location:** HKLM\Comm\SDCCF10G1\Parms\Configs\GlobalConfig
  **Key:** bLRS
  **Type:** DWORD

The channel map is a bitmap of 16 bits. The rightmost bit (bit 0) corresponds to channel 1; the next bit corresponds to channel 2, and so on.

The following table shows the channel maps and value for channels 2 and 9:

| Bit # | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | Registry Key Value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Channel # | N/A | N/A | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
| Value | N/A | N/A | 8192 | 4096 | 2048 | 1024 | 512 | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |
| Example | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 256+2=258 |

- **Communication problems with the Meru network:** When G rates are enabled and the Summit brand device is communicating, the Meru infrastructure sends beacon rates at what it perceives to be the connection rate. Because of this, the Summit 10 or 20 series radios may miss beacons from the Meru infrastructure. This communication issue does not occur when connecting with B rates only.
  Summit recommends the following settings when ou use a Meru network:
  - B rates only
  - CCX - Off
  - Aggressive Scanning - Off
- **Differences in Roaming Behavior:** Depending on the chipset, Summit brand radios may display different roaming behaviors. Some radios (such as the 30AG devices) send out a disassociation packet prior to roaming. Other radios (such as the 10/15/20 serues devices) do not; they simply drop association with no packet sent.
- **Startup Delays (EC25N):** To avoid potential start up delays, do not manually disable WZC.

## Revision History

| Revision | Date | Description | Initiated By |
|---|---|---|---|
| 1.0 | 29 Jan 2015 | Converted from HTML. Initial Release | Sue White |
| | | | |