



M9000

User Guide

Declarations of Conformity

Safety

Introduction

Key Combinations

Touchscreen

Software Keyboard

Display Rotation

Standby and Hibernation Functions

Saving Power

Security Measures

Battery Power

SD Memory Card

Wireless USB

Camera

Barcode Reader

Barcode Configuration Utility

Cradle

LAN

Wireless LAN

WWAN

Disabling / Enabling Wireless Communication???

Bluetooth

Zigbee Radio

Setup Utility (HCC?)

Hardware Diagnostics

Error Code / Message????

Technical Information

Troubleshooting????

Accessories

Software (OS)

Software (Apps)

Backpack Customization

Table of Contents

Table of Contents

1.0 Safety Information

1.1 User and Product Safety

- Do not stare into the laser or LED beam directly or shine it into eyes.
- Never use strong pressure onto the screen or subject it to severe impact, as the LCD panel could become cracked and possibility cause personal injury. If the LCD panel is broken, never touch the liquid inside because the liquid irritates the skin.
- Although the PDT has passed the test of IP65 standard for water and dust resistance, avoid prolonged exposure to rain or other concentrated moisture. Such condition exceeds the IP65 standard, and could result in water or other contaminants entering into the PDT.
- Use only the original approved AC Adapter with the PDT. Use of an unapproved AC Adapter could result in electrical problems, or even cause a fire or electrical shock to the user.
- Do not disassemble the PDT. Servicing should be done by supplier only. If the PDT or accessories gets damaged due to wrong handling or unauthorized repair, warranty is void. In case the warranty seals are broken, warranty is void too.
- Make regularly back-up of all important data.
- Under no circumstance will supplier be liable for any direct, indirect, consequential or incidental damages baring out of the use or inability to use the hardware and software and/or any data loss, even if supplier has been informed about the possibility of such damages.
- **LASER RADIATION: DO NOT STARE INTO BEAM CLASS 2 LASER PRODUCT.**



– RADIATION EXPOSURE STATEMENT –

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

1.2 Battery Safety



– WARNING –

Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Lithium-ion battery packs might get hot, explode, ignite and/or cause serious injury if exploded by abusive using. Please follow the safety warnings listed as below:

- Do not throw the battery pack in fire. Do not expose the battery to high temperatures.
- Do not connect the positive battery pack with negative battery pack to each other with any metal object (like wire).
- Do not carry or store battery pack together with metal objects.
- Do not pierce the battery pack with nails or drills, strike the battery pack with a hammer, step on the battery pack or otherwise expose it to strong impacts, shocks or excessive force.
- Do not solder onto the battery pack.
- Do not expose battery pack to liquid or allow the battery contacts to get wet.
- Do not disassemble or modify the battery pack. The battery pack contains safety and protection measures, which, if damaged, may cause the battery pack to generate heat, explode or ignite.
- Do not discharge the battery pack using any device except for the specified device. When it is used in devices other than the specified devices, the battery pack can be damaged or its life expectancy reduced. If the device causes any abnormal current to flow, it may cause the battery pack to become hot, explode or ignite and cause serious injury.
- In the event the battery pack leaks and the fluid gets into one's eye, do not rub the eye. Rinse well with water and immediately seek medical care. If left untreated, the battery fluid could cause damage to the eye.

2.3 LED and LASER Safety Information

- Class II LED/Laser Product
- Do not stare at the LED/Laser or shine into eyes
- Do not allow young children to use the product without adult supervision
- Do not replace/repair the LED/Laser, these are not user replaceable
- Do not shine the LED/Laser on a shiny reflective surface
- **LASER RADIATION DO NOT STARE INTO BEAM CLASS 2 LASER PRODUCT**

2.0 Conformity Statements

2.1 Warranty Statements

DAP Technologies makes no representation or warranty with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

The information in this manual is subject to change. DAP Technologies reserves the right to update and modify the M9000 Series, its accessories, and manuals without notice.

No part of this manual may be copied, distributed, transmitted, transcribed, stored in a retrieval system, or translated in any form or by any means, whether electronically or manually, without the express written consent of DAP Technologies.

As manufacturer, DAP Technologies will replace or repair, at its discretion, any products that prove to be defective in either materials or workmanship, for a period of one year following the purchase date of the M9000 Series unit and for a period of ninety (90) days following the purchase date of the M9000 accessories sold by DAP Technologies. The warranty only covers the materials and workmanship.

This warranty does not cover damages caused by misuse, abuse, or neglect, or occurring during shipping or storage; the warranty does not also cover any modification or servicing by anyone other than a DAP Technologies Authorized Service Center.

DAP Technologies cannot be held responsible for any damage caused by the misuse of the M9000 Series unit or by any other software or hardware added to the M9000.

The operating system, MS-DOS®, Windows CE, and all other software sold or supplied by DAP Technologies are provided as is, without any warranty, either express or implied.

In no event shall DAP Technologies be liable for any direct damage, indirect damage, or damage of any kind, including but not limited to damages on account of the loss of present or prospective profits arising out of or in connection with the use or failure of performance of this product. No claim may be made against DAP Technologies under this head, whether arising from contractual, extra-contractual, or statutory liability.

The warranty allowed hereby excludes all other legal warranties related to the quality of this product or its capacities to fulfill specific purposes, including all warranties granted by the United States Convention on Contracts for the International Sale of Goods, the application of such Convention being expressly excluded.

Revision April 2011

Printed in USA

M9010 is a registered trademark of DAP Technologies. Microsoft and MS-DOS® are registered trademarks of Microsoft Corporation.


2.2 FCC 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.

Complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

	– RADIATION EXPOSURE STATEMENT –
	<p>This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.</p> <p>This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.</p> <p>The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.</p>

2.3 Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003 and RSS210. 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.

This device has been designed to operate with the WWAN antenna having a maximum gain of 1.50 dB for the cellular band and 3.50 dB for the PCS band. WWAN antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The Required antenna impedance is 50 ohms.

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

2.0 Conformity Statements

2.4 Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2006 — Safety of Information Technology Equipment
- EN50371 : (2002-03) — Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (10 MHz - 300 GHz) -- General public
- EN 300 440-1 V1.4.1: (2008-05) — Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part1: Technical characteristics and test methods
- EN 300 440-2 V1.2.1: (2008-05) — Electromagnetic compatibility and radio spectrum matters (ERM); Wireless microphones in the 25 MHz to 3 GHz frequency range;
- EN 301 908-1 V3.2.1: (2007-05) — Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive
- EN 301 489-1 V1.8.1: (2008-04) — Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-3 V1.4.1 (2002-08) — Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz
- EN 301 489-7 V1.3.1 (2005-11) — Electromagnetic compatibility and Radio spectrum Matters -(ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- EN 301 489-17 V1.3.2 (2007-06) — Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wide-band transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz broadband data transmitting systems
- EN 301 489-19 V1.2.1 (2002-11) — Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 19: Specific conditions for Receive-Only Mobile Earth Stations (ROMES) operating in the 1,5 GHz band providing data communication
- EN 301 489-24 V1.5.1 (2010-10) — Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA and E-UTRA) for Mobile and portable (UE) radio and ancillary equipment
- EN 301 489-33 V1.1.1 (2009-02) — Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 33: Specific conditions for Ultra-Wide-Band (UWB) communications devices
- EN 302 065 V1.2.1 (2010-07) — Electromagnetic compatibility and Radio spectrum Matters (ERM); Short-Range Devices (SRD) using Ultra- Wide-Band technology (UWB) for communications purposes; Harmonised EN covering the essential requirements of Article 3.2 of the R&TTE Directive
- EN 301 511 V9.0.2 (2003-3) — Global System for Mobile communications (GSM); Harmonised EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under Article 3.2 of the R&TTE Directive (1999/5/EC)
- EN 301 893 V1.5.1 (2008-12) — Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonised EN covering the essential requirements of Article 3.2 of the R&TTE Directive
- EN 300 328 V1.7.1 (2006-02) — Electromagnetic compatibility and Radio spectrum Matters (ERM); Wide-band transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide-band modulation techniques; Harmonised EN covering essential requirements under Article 3.2 of the R&TTE Directive
- EN 62311:2008 — Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz-300 GHz)
- EN 55022:2006/A1:2007 — Information technology equipment — Radio disturbance characteristics — Limits and methods of measurement
- EN 55024:1998/A2:2003 — Information technology equipment — Immunity characteristics — Limits and methods of measurement

2.5 European Union CE Marking and Compliance Notices

Statements of Compliance:

English — This product follows the provisions of the European Directive 1999/5/EC.

Danish — Dette produkt er i overensstemmelse med det europæiske direktiv 1999/5/EC.

Dutch — Dit product is in navolging van de bepalingen van Europees Directief 1999/5/EC.

Finnish — Tämä tuote noudattaa EU-direktiivin 1999/5/EC määräyksiä.

French — Ce produit est conforme aux exigences de la Directive Européenne 1999/5/EC.

German — Dieses Produkt entspricht den Bestimmungen der Europäischen Richtlinie 1999/5/EC.

Greek — Το προϊόν αυτό πληροί τις προβλέψεις της Ευρωπαϊκής Οδηγίας 1999/5/EC.

Spanish — Este producto cumple las disposiciones de la Directiva Europea 1999/5/CE.

Specifications

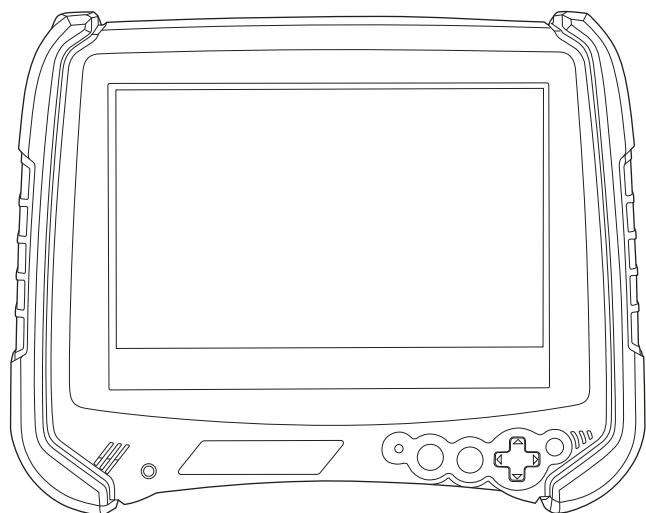
1.6 Specifications

Operating System	Windows® Embedded Standard 7, Windows® CE 6.0 Professional
Processor	Intel® Atom™ E660T 1.3 GHz
Memory	1 GB DDR2 SDRAM (2 GB optional)
Storage	16 GB solid state drive (32 or 64 GB optional)
Display	Sunlight-viewable Hardened touchscreen Landscape or portrait orientation Passive stylus or finger operation 7-inch WVGA (800 x 480) 550 nits
Sensors	Light sensor for auto backlight adjustment Position sensor (accelerometer) for portrait or landscape screen orientation
Keypad / Buttons	3-key keypad (enter, navigation, function) 7 programmable keys (touchscreen) Adjustable keypad backlight Programmable trigger on underside
Communications	WLAN — Summit 802.11 a/b/g/n WWAN — Gobi™ 3000: (CDMA, EVDO, UMTS, GSM, GPRS, EDGE, DTM, HSPA, 3G: 14.4 / 5.76 Mbps DOR: 9.3 / 5.4 Mbps) GPS — Gobi™ 3000 (Standalone, XTRA, AGPS) Zigbee® — Building Automation (BA) Home Automation (HA) Smart Energy (SE) Wireless USB — Video/data Bluetooth® — v2.1 + EDR Class II (BlueSoleil stack)
Input / Output	Power jack 1x RS-232 1x USB 2.0 Via dock connector: 1x USB 2.0 1x Ethernet
Barcode Scanning	Short range barcode: 1D laser Camera: 5-MP color camera with flash
Expansion Slots	SD card slot (supports up to 32 GB) Multi-I/O interface: 2x USB 2.0 1x CAN bus 2.0 (interface only) 1x SDVO (Serial Digital Video Out) 2x RS-232
Audio	Speaker Intel® HD Audio 3.2 mm stereo headset jack

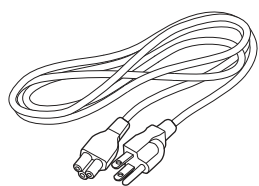
Software	Windows® Embedded 7: IE8, IIS 7.0, .NET 3.5, Remote Desktop, SQL, Backup and Restore, Boot from VHD or USB, Power Management, EWF and FBWF Windows® CE 6.0 Professional: ActiveSync, FTP client/server, IE 6.0, Viewers for Microsoft® Office and PDF files, Inbox, Windows Media Player, Remote Desktop, Terminal Services, Voice Recorder, Backup and Restore, Barcode Scanner Utility
Power	Primary internal: Li-ion battery, 7.4 V, 3000 mAh Secondary battery: Li-ion battery pack, 7.4 V, 3000 mAh Input: 10–20 VDC, 2 A
Dimensions & Weight	9.0 (L) x 7.3 (W) x 2.3 (H) inches [230 x 185 x 60 mm] 2.96 lb. [1346 g]
Regulatory	FCC Class B CE RoHS WEEE Laser safety: A21CFR1040.10 IEC/EN 60825-1
Environment	Operating temperature: -22 to +122 °F [-30 to +50 °C] Charging temperature: 32 to +104 °F [0 to +40 °C] Storage temperature: -22 to +158 °F [-30 to +70 °C] Drop: Multiple 6-foot (1.8-meter) drops to concrete ESD: 15 kV air discharge, 8 kV direct discharge Sealing: IP67 certified Humidity: 5%-95%, non-condensing Vibration: MIL-STD-810F

3.0 Getting Started

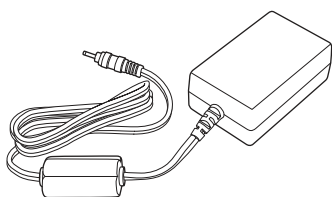
3.1 What's In the Package



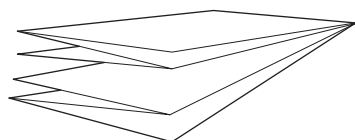
M9010



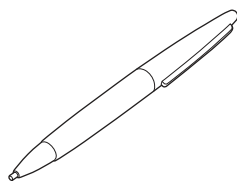
**Power Cords (US, UK,
and EU)**



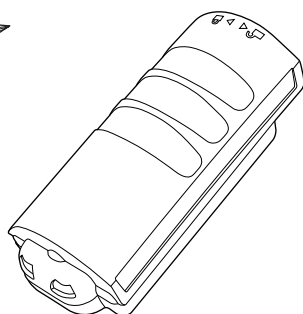
AC Adapter



Quick Start Guide



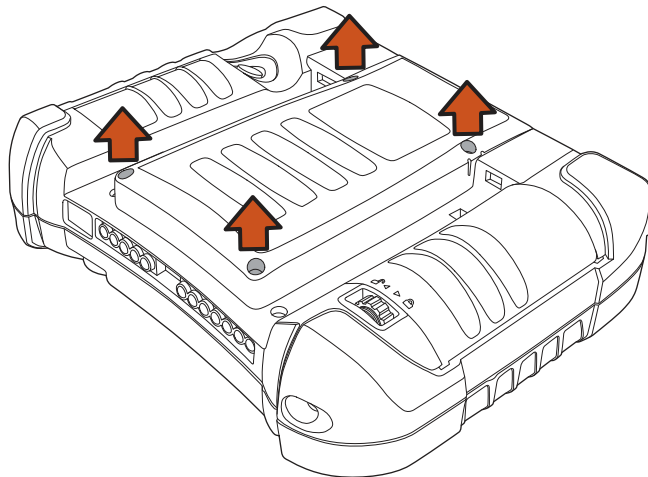
Stylus



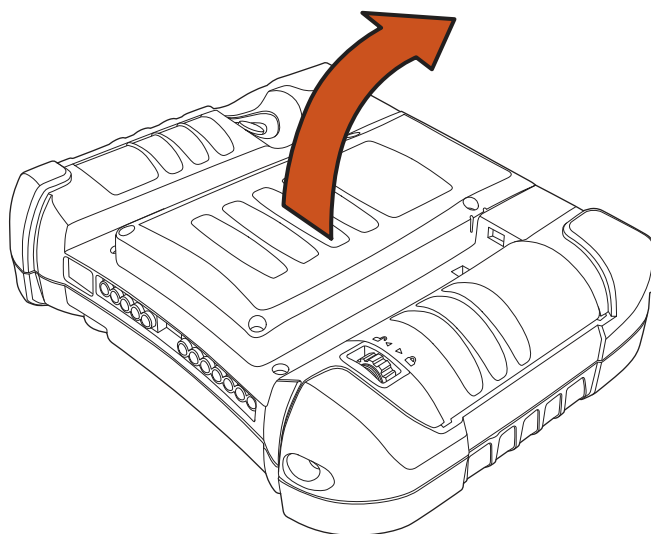
Battery Pack

3.2 Installing Optional Memory Cards

1. Using a flathead screwdriver, remove the screws as shown.

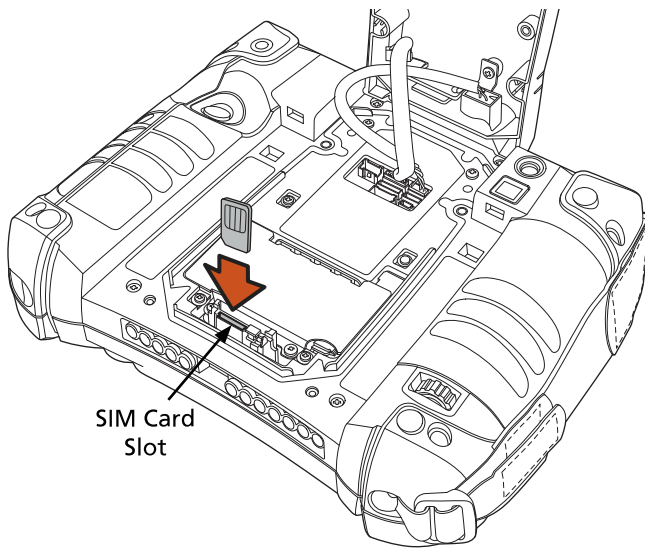


2. Lift the back cover off.

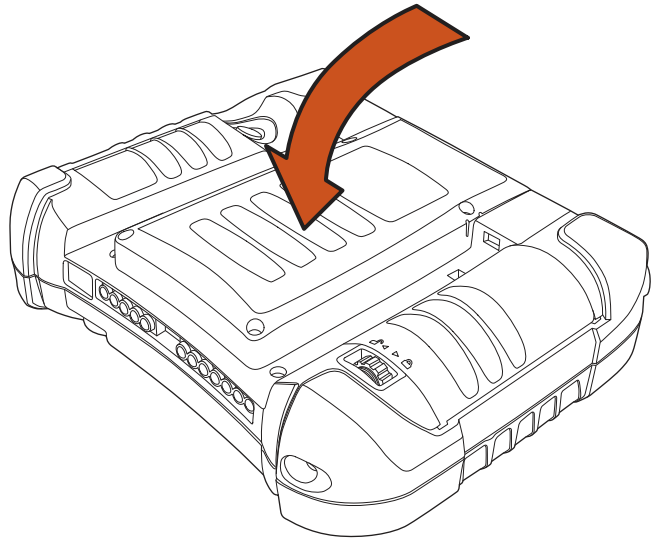


3.0 Getting Started (cont'd)

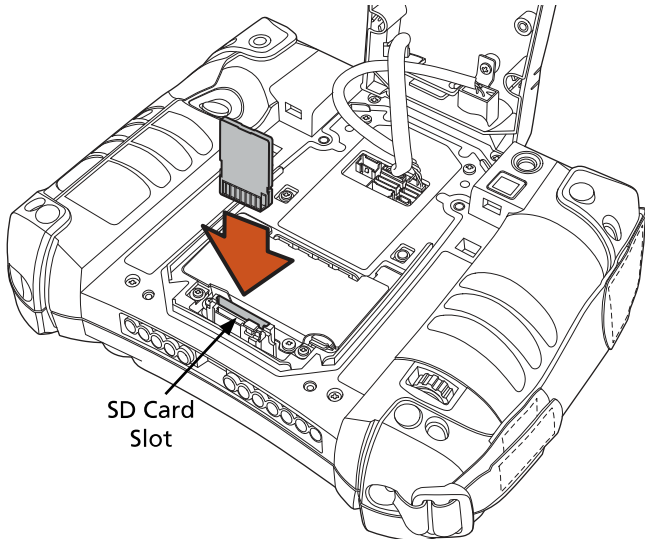
3. Insert the SIM Card into the small slot.



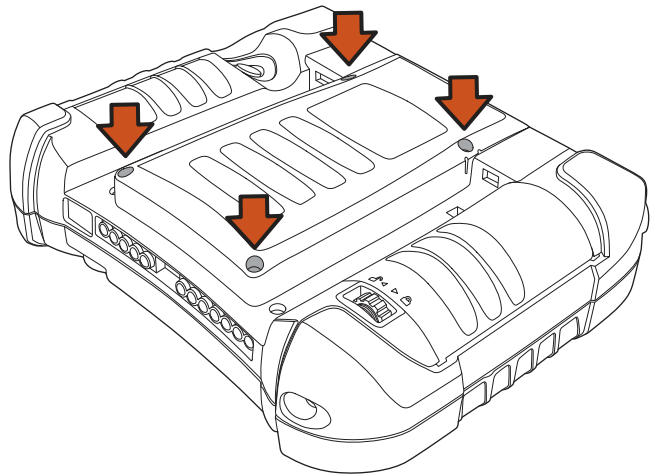
5. Place the cover back on the unit.



4. Insert the SD Card into the slot and press in until it locks in place.



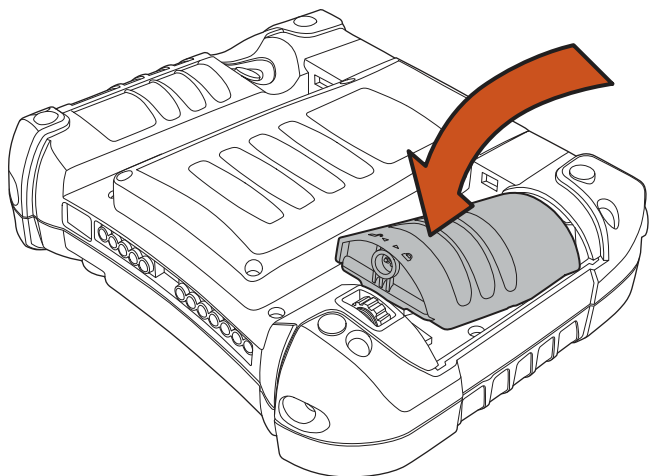
6. Insert the screws into their holes and tighten using a flathead screwdriver.



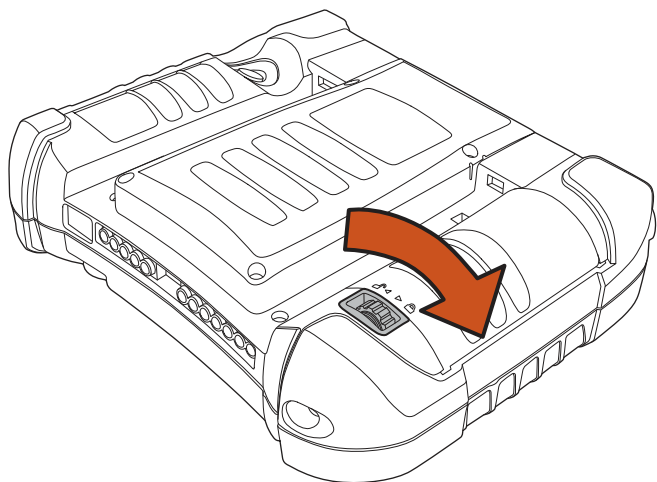
3.0 Getting Started (cont'd)

3.3 Install the Battery

1. Insert the battery as shown to the right.

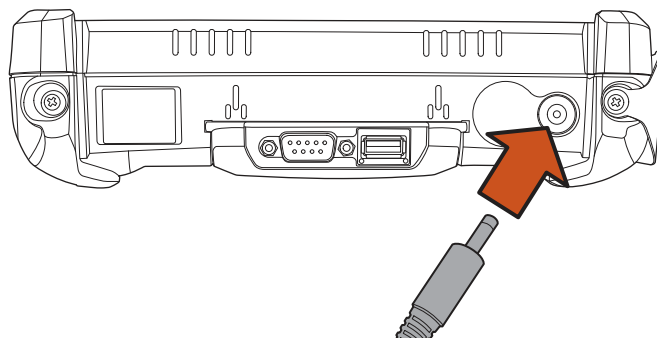


2. Turn the battery lock wheel clockwise until the battery is locked in place.

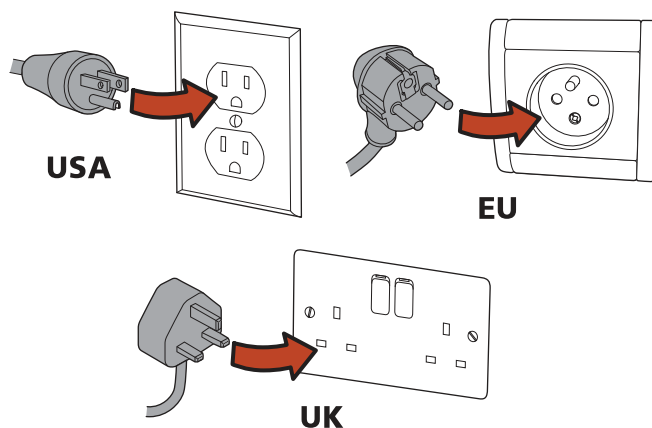


3.4 Charge the Battery

3. Insert the AC adapter into the power input.



4. Insert the power cord into the wall outlet and charge the battery for a minimum of 6 hours.

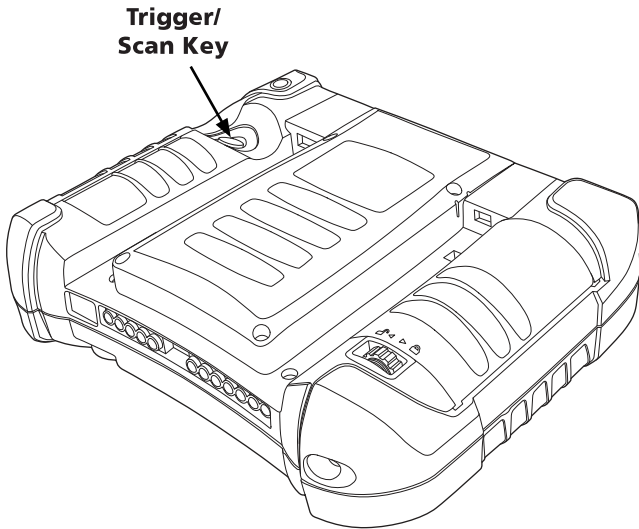


3.0 Getting Started (cont'd)

3.5 Operating the Unit

3.5.1 Turning the Unit On



1. Once the unit is charged, turn the unit on by pressing the trigger on the back of the unit.





2. A DAP splash screen will appear while the OS is loading.
3. Once the OS has loaded, the desktop will appear.
4. The unit is ready for use.

3.5.2 Launching an Application

3.5.2.1 Using the Stylus

1. Touch the Start Menu Icon  or Start Menu Button  with a finger or the stylus.
2. When the Start Menu appears, select an item to launch or navigate with using a finger or stylus.

3.5.3.2 Using the Nav Button

1. Touch the Start Menu Icon  or Start Menu Button  with a finger or a stylus.
2. Once the Start Menu appears, use the Nav Button to scroll the list of items.
3. To select a sub-menu, press the right side of the Nav Button. Pressing the left side of the Nav Button while in a sub-menu will take you to the previous menu.
4. Once an item to be selected is highlighted, press the Enter Button to launch the item.

3.5.3 Entering Data

1. Attach a keyboard to the USB connector on the back of the unit.

– OR –
2. Press the keyboard icon at the upper left of the desktop and pull to the right.
3. Release and a soft keyboard will appear on the screen.

3.5.4 Using the 1D Barcode Scanner

1. Launch the data capture application.
2. Aim the 1D Barcode Scanner at the barcode

Correct Scan:



Incorrect Scans:



NOTE: The laser must cross every bar simultaneously for the scanner to read the code.

3.0 Getting Started (cont'd)

3.0 Getting Started (cont'd)

1.5 Parameter Menus

This chapter describes the programmable parameters, provides bar codes for programming, and hexadecimal equivalents for host parameter programming through SSI.

Operational Parameters

The SE-955 is shipped with the factory default settings shown in Table 8-1 on page 8-5. These factory default values are stored in non-volatile memory and are preserved even when the scanner is powered down. Changes to the factory default values can be stored as custom defaults. These values are also stored in non-volatile memory and are preserved even when the scanner is powered down.

To change the parameter values:

- Scan the appropriate bar codes included in this chapter. The new values replace the existing memory values. To set the new values as custom defaults, scan the Write to Custom Defaults bar code. The factory default or custom default parameter values can be re-

called by scanning the SET FACTOR DEFAULT bar code or the RESTORE DEFAULTS bar code on page 8-10.

or

- Send the parameter through the scan engine's serial port using the SSI command PARAM_SEND. Hexadecimal parameter numbers are shown in this chapter below the parameter title, and options appear in parenthesis beneath the accompanying bar codes. Instructions for changing parameters using this method are found in Chapter 9, Simple Serial Interface.

The table below lists the factory defaults for all parameters. To change any option, scan the appropriate bar code(s).

Parameter	Parameter Number (Hex)	Factory Default	Page Number
Set Factory Default		All Defaults	8-10
Beeper Volume	0x8C	Medium	8-11
Beeper Tone	0x91	Medium Frequency	8-12
Beeper Frequency Adjustment	0xF0 0x91	2500 Hz	8-12
Laser On Time	0x88	3.0 sec	8-13
Aim Duration	0xED	0.0 sec	8-13
Scan Angle	0xBF	Medium (46°)	8-14
Power Mode	0x80	Low Power	8-14
Trigger Mode	0x8A	Level	8-16
Time-out Between Same Symbol	0x89	1.0 sec	8-17
Beep After Good Decode	0x38	Enable	8-17
Transmit "No Read" Message	0x5E	Disable	8-18
Parameter Scanning	0xEC	Enable	8-18
Linear Code Type Security Levels	0x4E	1	8-19
Linear Code Type Security Levels	0x4E	1	8-19
Bi-directional Redundancy	0x43	Disable	8-20
UPC/EAN			
UPC-A	0x01	Enable	8-21
UPC-E	0x02	Enable	8-21
UPC-E1	0x0C	Disable	8-22
EAN-8	0x04	Enable	8-22
EAN-13	0x03	Enable	8-23
Bookland EAN	0x53	Disable	8-23
Decode UPC/EAN Supplementals	0x10	Ignore	8-24
Decode UPC/EAN Supplemental Redundancy	0x50 7	8-25	
Transmit UPC-A Check Digit	0x28	Enable	8-26
Transmit UPC-E Check Digit	0x29	Enable	8-26
Transmit UPC-E1 Check Digit	0x2A	Enable	8-27
UPC-A Preamble	0x22	System Character	8-28

Parameter	Parameter No. (Hex)	Factory Default	Page No.
UPC-E Preamble	0x23	System Character	8-29
UPC-E1 Preamble	0x24	System Character	8-30
Convert UPC-E to A	0x25	Disable	8-31
Convert UPC-E1 to A	0x26	Disable	8-31
EAN-8 Zero Extend	0x27	Disable	8-32
Convert EAN-8 to EAN-13 Type	0xE0	Type is EAN-13	8-32
UPC/EAN Security Level	0x4D	0	8-33
UCC Coupon Extended Code	0x55	Disable	8-34
Code 128			
Code-128	0x08	Enable	8-35
UCC/EAN-128	0x0E	Enable	8-35
ISBT 128	0x54	Enable	8-36
Code 39			
Code 39	0x00	Enable	8-37
Trioptic Code 39	0x0D	Disable	8-37
Convert Code 39 to Code 32	0x56	Disable	8-38
Code 32 Prefix	0xE7	Disable	8-38
Set Length(s) for Code 39	0x12 0x13	2-55	8-39
Code 39 Check Digit Verification	0x30	Disable	8-40
Transmit Code 39 Check Digit	0x2B	Disable	8-40
Code 39 Full ASCII Conversion	0x11	Disable	8-41
Code 93			
Code 93	0x09	Disable	8-42
Set Length(s) for Code 93	0x1A 0x1B	4-55	8-43
Code 11			
Code 11	0x0A	Disable	8-44
Set Lengths for Code 11	0x1C 0x1D	4 to 55	8-44
Code 11 Check Digit Verification	0x34	Disable	8-46
Transmit Code 11 Check Digit(s)	0x2F	Disable	8-46
Interleaved 2 of 5			
Interleaved 2 of 5	0x06	Enable	8-48
Set Length(s) for I 2 of 5	0x16 0x17	14	8-49
I 2 of 5 Check Digit Verification	0x31	Disable	8-50
Transmit I 2 of 5 Check Digit	0x2C	Disable	8-51
Convert I 2 of 5 to EAN 13	0x52	Disable	8-51
Discrete 2 of 5			
Discrete 2 of 5	0x05	Disable	8-52
Set Length(s) for D 2 of 5	0x14 0x15	12	8-53
Chinese 2 of 5			
Chinese 2 of 5	0xF0 0x98	Disable	8-54

Parameter	Parameter No. (Hex)	Factory Default	Page No.
Codabar			
Codabar	0x07	Disable	8-55
Set Lengths for Codabar	0x18 0x19	5-55	8-56
CLSI Editing	0x36	Disable	8-57
NOTIS Editing	0x37	Disable	8-57
MSI			
MSI	0x0B	Disable	8-58
Set Length(s) for MSI	0x1E 0x1F	6-55	8-59
MSI Check Digits	0x32	One	8-60
Transmit MSI Check Digit	0x2E	Disable	8-60
MSI Check Digit Algorithm	0x33	Mod 10/Mod 10	8-61
RSS			
RSS-14	0xF0 0x52	Disable	8-62
RSS-Limited	0xF0 0x53	Disable	8-62
RSS-Expanded	0xF0 0x54	Disable	8-63
Data Options			
Transmit Code ID Character	0x2D	None	8-64
Prefix/Suffix Values			8-65
Prefix	0x69	NULL	
Suffix 1	0x68	LF	
Suffix 2	0x6A	CR	
Scan Data Transmission Format	0xEB	Data as is	8-66
Serial Interface			
Baud Rate	0x9C	9600	8-68
Parity	0x9E	None	8-70
Software Handshaking	0x9F	Enable	8-71
Decode Data Packet Format	0xEE	Unpacketed	8-72
Host Serial Response Time-out	0x9B	2 sec	8-72
Stop Bit Select	0x9D	1	8-73
Intercharacter Delay	0x6E	0	8-73
Host Character Time-out	0xEF	200 msec	8-73
Event Reporting*			
Decode Event 0xF0	0x00	Disable	8-74
Boot Up Event 0xF0	0x02	Disable	8-75
Parameter Event 0xF0	0x03	Disable	8-75
*See Table 9-9 on page 9-20 for formatting of any parameter whose number is 0x100 or greater.			

1.5.1 Set Default Parameter

The SE-955 can be reset to two types of defaults: factory defaults or custom defaults. Scan the appropriate bar code below to reset the SE-955 to its default settings and/or set the scanner's current settings as the custom default.

- **Restore Defaults** - Scan this bar code to reset all default parameters as follows.
 - If custom defaults were set by scanning **Write to Custom Defaults**, scan **Restore Defaults** to retrieve and restore the scanner's custom default settings.
 - If no custom defaults were set, scan **Restore Defaults** to restore the factory default values listed in Table 8-1 on page 8-5.



Restore Defaults

- **Set Factory Defaults** - Scan this bar code to restore the factory default values listed in Table 8-1 on page 8-5. If custom defaults were set, they are eliminated.



Set Factory Defaults

- **Write to Custom Defaults** - Scan this bar code to store the current scanner settings as custom defaults. Once custom default settings are stored, they can be recovered at any time by scanning **Restore Defaults**.



Write to Custom Defaults

1.5.2 Beeper Volume

Parameter # 0x8C

To select a decode beep volume, scan the appropriate bar code.



Low (0x02)



***Medium (0x01)**



High (0x00)

1.5.3 Beeper Tone

Parameter # 0x91

To select a decode beep frequency (tone), scan the appropriate bar code.



Low Frequency (0x02)



***Medium Frequency (0x01)**



High Frequency (0x00)

1.5.4 Beeper Frequency Adjustment

Parameter # 0xF0 0x91

This parameter adjusts the frequency of the high beeper tone from the nominal 2500 Hz to another frequency matching the resonances of the installation. It is programmable in 10 Hz increments from 1220 Hz to 3770 Hz.

To increase the frequency, scan the bar code below, then scan three numeric bar codes beginning on page 8-71 that correspond to the desired frequency adjustment divided by 10. For example, to set the frequency to 3000 Hz (an increase of 500 Hz), scan numeric bar codes 0, 5, 0, corresponding to 50, or (500/10).

To decrease the frequency, scan the bar code below, then scan three numeric bar codes beginning on page 8-71 that correspond to the value (256 - desired adjustment/10). For example, to set the frequency to 2000 Hz (a decrease of 500 Hz), scan numeric bar codes 2, 0, 6, corresponding to 206, or (256 - 500/10).

To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72.



**Beeper Frequency Adjustment
(Default: 2500 Hz)**

1.5.5 Laser On Time

Parameter # 0x88

This parameter sets the maximum time decode processing continues during a scan attempt. It is programmable in 0.1 second increments from 0.5 to 9.9 seconds.

To set a Laser On Time, scan the bar code below. Next scan two numeric bar codes beginning on page 8-71 that correspond to the desired on time. Single digit numbers must have a leading zero. For example, to set an on time of 0.5 seconds, scan the bar code below, then scan the “0” and “5” bar codes. To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72.



Laser On Time
(Default: 3.0 sec.)

1.5.6 Aim Duration

Parameter # 0xED

When a scanner with an aim mode (see Table 9-10 on page 9-22) is triggered either by a trigger pull, or a START_DECODE command, this parameter sets the duration the aiming pattern is seen before a scan attempt begins. It does not apply to the aim signal or the AIM_ON command. It is programmable in 0.1 second increments from 0.0 to 9.9 seconds. No aim pattern is visible when the value is 0.0. For more information on the use of this parameter, see the AIM_ON command on 9-6.

To set an aim duration, scan the bar code below. Next scan two numeric bar codes beginning on page 8-71 that correspond to the desired aim duration. Single digit numbers must have a leading zero. For example, to set an aim duration of 0.5 seconds, scan the bar code below, then scan the “0” and “5” bar codes. To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72.



Aim Duration
(Default: 0.0 sec.)

1.5.7 Scan Angle

Parameter # 0xBF

This parameter sets the scan angle to narrow, medium or wide.



Narrow Angle (35°)
(0x05)



***Medium Angle (46°)**
(0x06)



Wide Angle (53°)
(0x07)

1.5.8 Power Mode

Parameter # 0x80

This parameter determines the power mode of the engine.

In Low Power mode, the scanner enters into a low power consumption Sleep power state whenever possible (provided all WAKEUP commands have been released). See [Power Management on page 1-5](#).

In Continuous Power mode, the scan engine remains in the Awake state after each decode attempt (see [Power Management on page 1-5](#)).

The Sleep and Awake commands (see [SLEEP on page 9-27](#) and [WAKEUP on page 9-30](#)) can be used to change the power state in either the Low Power mode or the Continuous Power mode.



Continuous Power (0x00)



Low Power (0x01)

1.5.9 Triggering Modes

Parameter # 0x8A

Choose one of the options below to trigger the scan engine. Bar codes and option numbers are on the following page.

- **Scan (Level)** - A trigger pull activates the laser and decode processing. The laser remains on and decode processing continues until a trigger release, a valid decode, or the Laser On Time-out is reached.
- **Scan (Pulse)** - A trigger pull activates the laser and decode processing. The laser remains on and decode processing continues until a valid decode or the Laser On Time-out is reached.
- **Continuous** - The laser is always on and decoding.
- **Blink** - This trigger mode is used for triggerless operation. Scanning range is reduced in this mode. This mode cannot be used with scanners that support an aim mode (see [Table 9-10 on page 9-22](#)).
- **Host** - A host command issues the triggering signal. The scan engine interprets an actual trigger pull as a Level triggering option.



***Level (0X00)**



Pulse (0X02)



Continuous (0X04)



Blinking (0X07)



Host (0X08)

1.5.10 Time-out Between Same Symbol

Parameter # 0x89

When in Continuous triggering mode, this parameter sets the minimum time that must elapse before the scanner decodes a second bar code identical to one just decoded. This reduces the risk of accidentally scanning the same symbol twice. It is programmable in 0.1 second increments from 0.0 to 9.9 seconds.

To set a time-out between same symbol, scan the bar code below. Next scan two numeric bar codes beginning on page 8-71 that correspond to the desired time-out. Single digit values must have a leading zero. For example, to set a time-out of 0.5 seconds, scan the bar code below, then scan the “0” and “5” bar codes. To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72.



**Time-out Between Same Symbol
(Default: 1.0 sec.)**

1.5.11 Beep After Good Decode

Parameter # 0x38

Scan this symbol to set the scanner to beep after a good decode.



***Beep After Good Decode
(0x01)**

Scan this symbol to set the scanner not to beep after a good decode. The beeper still operates during parameter menu scanning and indicates error conditions.



**Do Not Beep After Good Decode
(0x00)**

1.5.12 Transmit “No Read” Message

Parameter # 0x5E

Enable this option to transmit “NR” if a symbol does not decode during the timeout period or before the trigger is released. Any enabled prefix or suffixes are appended around this message.



**Enable No Read
(0x01)**

When disabled, and a symbol cannot be decoded, no message is sent to the host.



***Disable No Read
(0x00)**

1.5.13 Parameter Scanning

Parameter # 0xEC

To disable decoding of parameter bar codes, scan the bar code below. The Set Defaults parameter bar code can still be decoded. To enable decoding of parameter bar codes, either scan *Enable Parameter Scanning (0x01), Set Factory Defaults or set this parameter to 0x01 via a serial command.



***Enable Parameter Scanning
(0x01)**



**Disable Parameter Scanning
(0x00)**

1.5.14 Linear Code Type Security Level

Parameter # 0x4E

The SE-955 offers four levels of decode security for linear code types (e.g. Code 39, Interleaved 2 of 5). Select higher security levels for decreasing levels of bar code quality. As security levels increase, the scanner's aggressiveness decreases. Select the security level appropriate for your bar code quality.

Linear Security Level 1

The following code types must be successfully read twice before being decoded:

Code Type	Length
Codabar	All
MSI	4 or less
D 2 of 5	8 or less
I 2 of 5	8 or less



***Linear Security Level 1
(0x01)**

Linear Security Level 2

All code types must be successfully read twice before being decoded.



**Linear Security Level 2
(0x02)**

Linear Security Level 3

Code types other than the following must be successfully read twice before being decoded. The following codes must be read three times:

Code Type	Length
MSI	4 or less
D 2 of 5	8 or less
I 2 of 5	8 or less



**Linear Security Level 3
(0x03)**

Linear Security Level 4

All code types must be successfully read three times before being decoded.



**Linear Security Level 4
(0x04)**

1.5.15 Bi-directional Redundancy

Parameter # 0x43

Enable this option to transmit "NR" if a symbol does not decode during the timeout period or before the trigger is released. Any enabled prefix or suffixes are appended around this message.



**Enable Bi-directional Redundancy
(0x01)**

When disabled, and a symbol cannot be decoded, no message is sent to the host.



***Disable Bi-directional Redundancy
(0x00)**

UPC / EAN

1.5.16 Enable/Disable UPC-A

Parameter # 0x01

To enable or disable UPC-A, scan the appropriate bar code below.



***Enable UPC-A
(0x01)**



**Disable UPC-A
(0x00)**

1.5.17 Enable/Disable UPC-E

Parameter # 0x02

To enable or disable UPC-E, scan the appropriate bar code below.



***Enable UPC-E
(0x01)**



**Disable UPC-E
(0x00)**

1.5.18 Enable/Disable UPC-E1

Parameter # 0x0C

To enable or disable UPC-E1, scan the appropriate bar code below.



**Enable UPC-E1
(0x01)**



***Disable UPC-E1
(0x00)**



UPC-E1 is not a UCC (Uniform Code Council) approved symbology.

1.5.19 Enable/Disable EAN-8

Parameter # 0x04

To enable or disable EAN-8, scan the appropriate bar code below.



***Enable EAN-8
(0x01)**



**Disable EAN-8
(0x00)**

1.5.19 Enable/Disable EAN-13

Parameter # 0x03

To enable or disable EAN-13, scan the appropriate bar code below.



***Enable EAN-13
(0x01)**



**Disable EAN-13
(0x00)**



UPC-E1 is not a UCC (Uniform Code Council) approved symbology.

1.5.20 Enable/Disable Bookland EAN

Parameter # 0x53

To enable or disable EAN Bookland, scan the appropriate bar code below.



**Enable Bookland EAN
(0x01)**



***Disable Bookland EAN
(0x00)**

1.5.21 Decode UPC/EAN Supplementals

Parameter # 0x10

Supplementals are appended characters (2 or 5) according to specific code format conventions (e.g., UPC A+2, UPC E+2). Several options are available:

- If Decode UPC/EAN with Supplemental characters is selected, the scanner does not decode UPC/EAN symbols without supplemental characters.
- If Ignore UPC/EAN with Supplemental characters is selected, and the SE-955 is presented with a UPC/EAN symbol with a supplemental, the scanner decodes the UPC/EAN and ignores the supplemental characters.
- If Autodiscriminate UPC/EAN Supplementals is selected, scan Decode UPC/EAN Supplemental Redundancy on page 8-25, then select a value from the numeric bar codes beginning on page 8-71. A value of 5 or more is recommended.
- Select Enable 378/379 Supplemental Mode to enable the SE-955 to identify supplementals for EAN-13 bar codes starting with a '378' or '379' prefix only. All other UPC/EAN bar codes are decoded immediately and the supplemental characters ignored.
- Select Enable 978 Supplemental Mode to enable the SE-955 to identify supplementals for EAN-13 bar codes starting with a '978' prefix only. All other UPC/EAN bar codes are decoded immediately and the supplemental characters ignored.
- Select Enable Smart Supplemental Mode to enable the SE-955 to identify supplementals for EAN-13 bar codes starting with a '378', '379', or '978' prefix only. All other UPC/EAN bar codes are decoded immediately and the supplemental characters ignored.



To minimize the risk of invalid data transmission, we recommend selecting whether to read or ignore supplemental characters.

To enable or disable EAN-13, scan the appropriate bar code below.



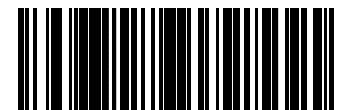
**Decode UPC/EAN With Supplementals
(0x01)**



***Ignore UPC/EAN With Supplementals
(0x00)**



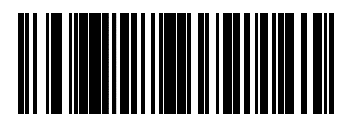
**Autodiscriminate UPC/EAN Supplementals
(0x02)**



**Enable 378/379 Supplemental Mode
(0x04)**



**Enable 978 Supplemental Mode
(0x05)**



**Enable Smart Supplemental Mode
(0x03)**

1.5.22 Decode UPC/EAN Supplemental Redundancy

Parameter # 0x50

With Autodiscriminate UPC/EAN Supplementals selected, this option adjusts the number of times a symbol without supplementals will be decoded before transmission. The range is from 2 to 30 times. Five or above is recommended when decoding a mix of UPC/EAN symbols with and without supplementals, and the autodiscriminate option is selected.

Scan the bar code below to select a decode redundancy value. Next scan two numeric bar codes beginning on page 8-71. Single digit numbers must have a leading zero. To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72.



Decode UPC/EAN Supplemental Redundancy
(Default: 7)

1.5.23 Transmit UPC-A Check Digit

Parameter # 0x28

Scan the appropriate bar code below to transmit the symbol with or without the UPC-A check digit.



***Transmit UPC-A Check Digit**
(0x01)



Do Not Transmit UPC-A Check Digit
(0x00)

1.5.24 Transmit UPC-E Check Digit

Parameter # 0x29

Scan the appropriate bar code below to transmit the symbol with or without the UPC-E check digit.



***Transmit UPC-E Check Digit**
(0x01)



Do Not Transmit UPC-E Check Digit
(0x00)

1.5.25 Transmit UPC-E1 Check Digit

Parameter # 0x2A

Scan the appropriate bar code below to transmit the symbol with or without the UPC-E1 check digit.



***Transmit UPC-A Check Digit**
(0x01)



Do Not Transmit UPC-A Check Digit
(0x00)

1.5.26 UPC-A Preamble

Parameter # 0x22

Preamble characters (Country Code and System Character) can be transmitted as part of a UPC-A symbol. Select one of the following options for transmitting UPC-A preamble to the host device: transmit system character only, transmit system character and country code ("0" for USA), or transmit no preamble.



No Preamble
(**<DATA>**)
(0x00)



***System Character**
(**<SYSTEM CHARACTER> <DATA>**)
(0x01)



System Character & Country Code
(**< COUNTRY CODE> <SYSTEM CHARACTER> <DATA>**)
(0x02)

1.5.27 UPC-E Preamble

Parameter # 0x23

Preamble characters (Country Code and System Character) can be transmitted as part of a UPC-E symbol. Select one of the following options for transmitting UPC-E preamble to the host device: transmit system character only, transmit system character and country code ("0" for USA), or transmit no preamble.



No Preamble
(<DATA>)
(0x00)



***System Character**
(<SYSTEM CHARACTER> <DATA>)
(0x01)



System Character & Country Code
(< COUNTRY CODE> <SYSTEM CHARACTER> <DATA>)
(0x02)

1.5.28 UPC-E1 Preamble

Parameter # 0x24

Preamble characters (Country Code and System Character) can be transmitted as part of a UPC-E1 symbol. Select one of the following options for transmitting UPC-E1 preamble to the host device: transmit system character only, transmit system character and country code ("0" for USA), or transmit no preamble.



No Preamble
(<DATA>)
(0x00)



***System Character**
(<SYSTEM CHARACTER> <DATA>)
(0x01)



System Character & Country Code
(< COUNTRY CODE> <SYSTEM CHARACTER> <DATA>)
(0x02)

1.5.29 Convert UPC-E to UPC-A

Parameter # 0x25

Enable this parameter to convert UPC-E (zero suppressed) decoded data to UPC-A format before transmission. After conversion, data follows UPC-A format and is affected by UPC-A programming selections (e.g., Preamble, Check Digit).

Scan **DO NOT CONVERT UPC-E TO UPC-A** to transmit UPC-E (zero suppressed) decoded data.



Convert UPC-E to UPC-A (Enable)
(0x01)



***Do Not Convert UPC-E to UPC-A (Disable)**
(0x00)

1.5.30 Convert UPC-E1 to UPC-A

Parameter # 0x26

Enable this parameter to convert UPC-E1 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, data follows UPC-A format and is affected by UPC-A programming selections (e.g., Preamble, Check Digit).

Scan **DO NOT CONVERT UPC-E TO UPC-A** to transmit UPC-E1 (zero suppressed) decoded data.



Convert UPC-E1 to UPC-A (Enable)
(0x01)



***Do Not Convert UPC-E1 to UPC-A (Disable)**
(0x00)

1.5.31 EAN Zero Extend

Parameter # 0x27

When enabled, this parameter adds five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols.

Disable this parameter to transmit EAN-8 symbols as is.



**Enable EAN Zero Extend
(0x01)**



***Disable EAN Zero Extend
(0x00)**

1.5.32 Convert EAN-8 to EAN-13 Type

Parameter # 0xE0

When EAN Zero Extend is enabled, you can label the extended symbol as either an EAN-13 bar code, or an EAN-8 bar code. This affects **Transmit Code ID Character** and **DECODE_DATA** message.

When EAN Zero Extend is disabled, this parameter has no effect on bar code data.



***Type Is EAN-13
(0x00)**



**Type Is EAN-8
(0x01)**

1.5.33 UPC/EAN Security Level

Parameter # 0x4D

The SE-955 offers four levels of decode security for UPC/EAN bar codes. Increasing levels of security are provided for decreasing levels of bar code quality. Select higher levels of security for decreasing levels of bar code quality. Increasing security decreases the scanner's aggressiveness, so choose only that level of security necessary for the application.

UPC/EAN Security Level 0: This default setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most "in-spec" UPC/EAN bar codes.



***UPC/EAN Security Level 0
(0x00)**

UPC/EAN Security Level 1: As bar code quality levels diminish, certain characters become prone to mis-decodes before others (i.e., 1, 2, 7, 8). If mis-decodes of poorly printed bar codes occur, and the mis-decodes are limited to these characters, select this security level.



**UPC/EAN Security Level 1
(0x01)**

UPC/EAN Security Level 2: If mis-decodes of poorly printed bar codes occur, and the mis-decodes are not limited to characters 1, 2, 7, and 8, select this security level.



**UPC/EAN Security Level 2
(0x02)**

UPC/EAN Security Level 3: If misdecodes still occur after selecting Security Level 2, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec bar codes. Selection of this level of security significantly impairs the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the bar codes.



**UPC/EAN Security Level 3
(0x03)**

1.5.34 UCC Coupon Extended Code

Parameter # 0x55

The UCC Coupon Extended Code is an additional bar code adjacent to a UCC Coupon Code. To enable or disable UCC Coupon Extended Code, scan the appropriate bar code below.



**Enable UCC Coupon Extended Code
(0x01)**



***Disable UCC Coupon Extended Code
(0x00)**

Code 128

1.5.35 Enable/Disable Code 128

Parameter # 0x08

To enable or disable Code 128, scan the appropriate bar code below.



***Enable Code 128
(0x01)**



**Disable Code 128
(0x00)**

1.5.36 Enable/Disable UCC/EAN-128

Parameter # 0x0E

To enable or disable UCC/EAN-128, scan the appropriate bar code below. (See **Chapter B, Miscellaneous Code Information** for details on UCC/EAN-128.)



***Enable UCC/EAN-128
(0x01)**



**Disable UCC/EAN-128
(0x00)**

1.5.37 Enable/Disable ISBT 128

Parameter # 0x54

To enable or disable ISBT 128, scan the appropriate bar code below.



***Enable ISBT 128
(0x01)**



**Disable ISBT 128
(0x00)**

1.5.38 Lengths for Code 128

No length setting is required for Code 128.

Code 39

1.5.39 Enable/Disable Code 39

Parameter # 0x00

To enable or disable Code 39, scan the appropriate bar code below.



***Enable Code 39
(0x01)**



**Disable Code 39
(0x00)**

1.5.40 Enable/Disable Trioptic Code 39

Parameter # 0x0D

Trioptic Code 39 is a variant of Code 39 used in marking computer tape cartridges. Trioptic Code 39 symbols always contain six characters.

To enable or disable Trioptic Code 39, scan the appropriate bar code below.



**Enable Trioptic Code 39
(0x01)**



***Disable Trioptic Code 39
(0x00)**



Note

Trioptic Code 39 and Code 39 Full ASCII cannot be enabled simultaneously. If an error beep sounds when enabling Trioptic Code 39, disable Code 39 Full ASCII and try again.

1.5.41 Convert Code 39 to Code 32 (Italian Pharma Code)

Parameter # 0x56

Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32.



Note

Code 39 must be enabled in order for this parameter to function.



**Enable Convert Code 39 to Code 32
(0x01)**



***Disable Convert Code 39 to Code 32
(0x00)**

1.5.42 Code 32 Prefix

Parameter # 0xE7

Enable this parameter to add the prefix character “A” to all Code 32 bar codes. **Convert Code 39 to Code 32 (Italian Pharma Code)** must be enabled for this parameter to function.



**Enable Code 32 Prefix
(0x01)**



***Disable Code 32 Prefix
(0x00)**

1.5.43 Set Lengths for Code 39

Parameter # L1 = 0x12, L2 = 0x13

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Lengths for Code 39 may be set for any length, one or two discrete lengths, or lengths within a specific range. If Code 39 Full ASCII is enabled, **Length Within a Range** or **Any Length** are the preferred options. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands on page B-8**.



When setting lengths, single digit numbers must always be preceded by a leading zero.

- **One Discrete Length** - This option limits decodes to only those Code 39 symbols containing a selected length. Lengths are selected from the numeric bar codes beginning on page 8-71. For example, to decode only Code 39 symbols with 14 characters, scan **Code 39 - One Discrete Length**, then scan **1** followed by **4**. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Code 39 - One Discrete Length

- **Two Discrete Lengths** - This option limits decodes to only those Code 39 symbols containing either of two selected lengths. Lengths are selected from the numeric bar codes beginning on page 8-71. For example, to decode only those Code 39 symbols containing either 2 or 14 characters, scan **Code 39 - Two Discrete Lengths**, then scan **0, 2, 1** and then **4**. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Code 39 - Two Discrete Lengths

- **Length Within Range** - This option limits decodes to only those Code 39 symbols within a specified range. For example, to decode Code 39 symbols containing between 4 and 12 characters, first scan **Code 39 - Length Within Range**. Then scan **0, 4, 1** and **2**. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Code 39 - Length Within Range

- **Any Length** - Scan this option to decode Code 39 symbols containing any number of characters.



Code 39 - Any Length

1.5.44 Code 39 Check Digit Verification

Parameter # 0x30

When this feature is enabled, the scanner checks the integrity of all Code 39 symbols to verify that the data complies with specified check digit algorithm. Only those Code 39 symbols which include a modulo 43 check digit are decoded. Only enable this feature if your Code 39 symbols contain a modulo 43 check digit.



**Verify Code 39 Check Digit
(0x01)**



***Do Not Verify Code 39 Check Digit
(0x00)**

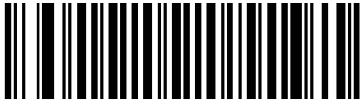
Code 39

Code 93

1.5.45 Transmit Code 39 Check Digit

Parameter # 0x2B

Scan this symbol to transmit the check digit with the data.



Verify Code 39 Check Digit
(0x01)

Scan this symbol to transmit data without the check digit.



*Do Not Verify Code 39 Check Digit
(0x00)

1.5.46 Enable/Disable Code 39 Full ASCII

Parameter # 0x11

Code 39 Full ASCII is a variant of Code 39 which pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII, scan the appropriate bar code below.

Refer to Table B-3 on page B-5 for the mapping of Code 39 characters to ASCII values.



Verify Code 39 Check Digit
(0x01)



*Do Not Verify Code 39 Check Digit
(0x00)



Trioptic Code 39 and Code 39 Full ASCII cannot be enabled simultaneously. If you get an error beep when enabling Code 39 Full ASCII, disable Trioptic Code 39 and try again.

1.5.47 Enable/Disable Code 93

Parameter # 0x00

To enable or disable Code 93, scan the appropriate bar code below.



Enable Code 93
(0x01)



*Disable Code 93
(0x00)

1.5.48 Set Lengths for Code 93

Parameter # L1 = 0x1A, L2 = 0x1B

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Lengths for Code 93 may be set for any length, one or two discrete lengths, or lengths within a specific range. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands** on page B-8.

- **One Discrete Length** - Select this option to decode only those codes containing a selected length. For example, select **Code 93 - One Discrete Length**, then scan **1, 4** to limit the decoding to only Code 93 symbols containing 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Code 93 - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only those codes containing two selected lengths. For example, select **Code 39 - Two Discrete Lengths**, then scan **0, 2, 1, 4** to limit the decoding to only Code 93 symbols containing 2 or 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Code 93 - Two Discrete Lengths

- **Length Within Range** - This option sets the unit to decode a code type within a specified range. For example, to decode Code 93 symbols containing between 4 and 12 characters, first scan **Code 39 - Length Within Range**. Then scan **0, 4, 1** and **2** (single digit numbers must always be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan Cancel on page 8-72.



Code 93 - Length Within Range

- **Any Length** - Scan this option to decode Code 93 symbols containing any number of characters.



Code 93 - Any Length

Code 11

1.5.49 Enable/Disable Code 11

Parameter # 0x0A

To enable or disable Code 11, scan the appropriate bar code below.



**Enable Code 11
(0x01)**



***Disable Code 11
(0x00)**

1.5.50 Set Lengths for Code 11

Parameter # L1 = 0x1C, L2 = 0x1D

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Set lengths for Code 11 to any length, one or two discrete lengths, or lengths within a specific range.

- **One Discrete Length** - Select this option to decode only Code 11 symbols containing a selected length. Select the length using the numeric bar codes in Numeric Bar Codes on page 8-76. For example, to decode only Code 11 symbols with 14 characters, scan **Code 11 - One Discrete Length**, then scan **1** followed by **4**. To correct an error or to change the selection, scan **Cancel** on page 8-77.



Code 11 - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only Code 11 symbols containing either of two selected lengths. Select lengths using the numeric bar codes in Numeric Bar Codes on page 8-76. For example, to decode only those Code 11 symbols containing either 2 or 14 characters, select **Code 11 - Two Discrete Lengths**, then scan **0, 2, 1**, and then **4**. To correct an error or to change the selection, scan **Cancel** on page 8-77.



Code 11 - Two Discrete Lengths

Length Within Range - Select this option to decode a Code 11 symbol with a specific length range. Select lengths using numeric bar codes in Numeric Bar Codes on page 8-76. For example, to decode Code 11 symbols containing between 4 and 12 characters, first scan **Code 11 - Length Within Range**. Then scan **0, 4, 1,** and **2** (single digit numbers must always be preceded by a leading zero). To correct an error or change the selection, scan **Cancel** on page 8-72.



Code 11 - Length Within Range

Any Length - Scan this option to decode Code 11 symbols containing any number of characters within the scanner capability.



Code 11 - Any Length

1.5.51 Code 11 Check Digit Verification

Parameter # 0x34

This feature allows the scanner to check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 bar code. The options are to check for one check digit, check for two check digits, or disable the feature.

To enable this feature, scan the bar code below corresponding to the number of check digits encoded in your Code 11 symbols.



***Disable
(0x00)**



**One Check Digit
(0x01)**



**Two Check Digits
(0x02)**

1.5.52 Transmit Code 11 Check Digits

Parameter # 0x2F

This feature selects whether or not to transmit the Code 11 check digit(s).



**Transmit Code 11 Check Digit(s) (Enable)
(0x01)**



***Do Not Transmit Code 11 Check Digit(s) (Disable)
(0x00)**



Code 11 Check Digit Verification must be enabled for this parameter to function.

Interleaved 2 of 5

1.5.53 Enable/Disable Interleaved 2 of 5

Parameter # 0x06

To enable or disable Interleaved 2 of 5, scan the appropriate bar code below.



***Enable Interleaved 2 of 5
(0x01)**



**Disable Interleaved 2 of 5
(0x00)**

1.5.54 Set Lengths for Interleaved 2 of 5

Parameter # L1 = 0x16, L2 = 0x17

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Lengths for I 2 of 5 may be set for any length, one or two discrete lengths, or lengths within a specific range. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands on page B-8**.



When setting lengths, single digit numbers must always be preceded by a leading zero.

- **One Discrete Length** - Select this option to decode only those codes containing a selected length. For example, select **I 2 of 5 - One Discrete Length**, then scan **1, 4**, to decode only I 2 of 5 symbols containing 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



I 2 of 5 - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only those codes containing two selected lengths. For example, select **I 2 of 5 - Two Discrete Lengths**, then scan **0, 6, 1, 4** to decode only I 2 of 5 symbols containing 6 or 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



I 2 of 5 - Two Discrete Lengths

- **Length Within Range** - Select this option to decode only codes within a specified range. For example, to decode I 2 of 5 symbols containing between 4 and 12 characters, first scan **I 2 of 5 - Length Within Range**. Then scan **0, 4, 1** and **2** (single digit numbers must always be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



I 2 of 5 - Length Within Range

- **Any Length** - Scan this option to decode Code 39 symbols containing any number of characters.



Selecting this option may lead to misdecodes for I 2 of 5 codes.



I 2 of 5 - Any Length

1.5.55 I 2 of 5 Check Digit Verification

Parameter # 0x31

When enabled, this parameter checks the integrity of an I 2 of 5 symbol to ensure it complies with a specified algorithm, either USS (Uniform Symbology Specification), or OPCC (Optical Product Code Council).



***Disable
(0x00)**



**USS Check Digit
(0x01)**



**OPCC Check Digit
(0x02)**

Discrete 2 of 5

1.5.56 Transmit I 2 of 5 Check Digit

Parameter # 0x2C

Scan this symbol to transmit the check digit with the data.



Transmit I 2 of 5 Check Digit (Enable)
(0x01)

Scan this symbol to transmit data without the check digit.



***Do Not Transmit I 2 of 5 Check Digit (Disable)**
(0x00)

1.5.57 Convert I 2 of 5 to EAN-13

Parameter # 0x52

This parameter converts a 14 character I 2 of 5 code into EAN-13, and transmits to the host as EAN-13. To accomplish this, I 2 of 5 must be enabled, one length must be set to 14, and the code must have a leading zero and a valid EAN-13 check digit.



Convert I 2 of 5 to EAN-13 (Enable)
(0x01)



***Do Not Convert I 2 of 5 to EAN-13 (Disable)**
(0x00)

1.5.58 Enable/Disable Discrete 2 of 5

Parameter # 0x05

To enable or disable Discrete 2 of 5, scan the appropriate bar code below.



Enable Discrete 2 of 5
(0x01)



***Disable Discrete 2 of 5**
(0x00)

1.5.59 Set Lengths for Discrete 2 of 5

Parameter # L1 = 0x14, L2 = 0x15

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Lengths for D 2 of 5 may be set for any length, one or two discrete lengths, or lengths within a specific range. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands** on page B-8.

- **One Discrete Length** - Select this option to decode only those codes containing a selected length. For example, select **D 2 of 5 - One Discrete Length**, then scan **1, 4**, to decode only D 2 of 5 symbols containing 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



D 2 of 5 - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only those codes containing two selected lengths. For example, select **D 2 of 5 - Two Discrete Lengths**, then scan **0, 4, 1, 2** (single digit numbers must be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



D 2 of 5 - Two Discrete Lengths

Chinese 2 of 5

- **Length Within Range** - Select this option to decode only codes within a specified range. For example, to decode D 2 of 5 symbols containing between 4 and 12 characters, first scan **D 2 of 5 - Length Within Range**. Then scan **0, 4, 1** and **2** (single digit numbers must always be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan Cancel on page 8-72.



D 2 of 5 - Length Within Range

- **Any Length** - Scan this option to decode D 2 of 5 symbols containing any number of characters.



Selecting this option may lead to misdecodes for D 2 of 5 codes.



D 2 of 5 - Any Length

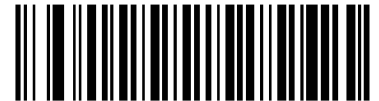
1.5.60 Enable/Disable Chinese 2 of 5

Parameter # 0xF0 0x98

To enable or disable Chinese 2 of 5, scan the appropriate bar code below.



**Enable Chinese 2 of 5
(0x01)**



***Disable Chinese 2 of 5
(0x00)**

Codabar

1.5.61 Enable/Disable Codabar

Parameter # 0x07

To enable or disable Codabar, scan the appropriate bar code below.



**Enable Codabar
(0x01)**



***Disable Codabar
(0x00)**

1.5.62 Set Lengths for Codabar

Parameter # L1 = 0x18, L2 = 0x19

The length of a code refers to the number of characters (i.e., human readable characters), including check digit(s) the code contains. Lengths for Codabar may be set for any length, one or two discrete lengths, or lengths within a specific range. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands on page B-8**.

- **One Discrete Length** - Select this option to decode only those codes containing a selected length. For example, select **Codabar - One Discrete Length**, then scan **1, 4**, to decode only Codabar symbols containing 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Codabar - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only those codes containing two selected lengths. For example, select **Codabar - Two Discrete Lengths**, then scan **0, 2, 1, 4** to decode only Codabar symbols containing 6 or 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Codabar - Two Discrete Lengths

- **Length Within Range** - Select this option to decode only codes within a specified range. For example, to decode D 2 of 5 symbols containing between 4 and 12 characters, first scan **D 2 of 5 - Length Within Range**. Then scan **0, 4, 1 and 2** (single digit numbers must always be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



Codabar - Length Within Range

- **Any Length** - Scan this option to decode D 2 of 5 symbols containing any number of characters.



Selecting this option may lead to misdecodes for D 2 of 5 codes.



Codabar - Any Length

1.5.63 CLSI Editing

Parameter # 0x36

When enabled, this parameter strips the start and stop characters and inserts a space after the first, fifth, and tenth characters of a 14-character Codabar symbol.



Symbol length does not include start and stop characters.



**Enable CLSI Editing
(0x01)**



***Disable CLSI Editing
(0x00)**

1.5.64 NOTIS Editing

Parameter # 0x37

When enabled, this parameter strips the start and stop characters from decoded Codabar symbol.



**Enable NOTIS Editing
(0x01)**



***Disable NOTIS Editing
(0x00)**

MSI

1.5.65 Enable/Disable MSI

Parameter # 0x0B

To enable or disable MSI, scan the appropriate bar code below.



Enable MSI
(0x01)



*Disable MSI
(0x00)

1.5.66 Set Lengths for MSI

Parameter # L1 = 0x1E, L2 = 0x1F

The length of a code refers to the number of characters (i.e., human readable characters) the code contains, and includes check digits. Lengths for MSI can be set for any length, one or two discrete lengths, or lengths within a specific range. See Table B-5 on page B-9 for ASCII equivalents. To set lengths via serial commands, see **Setting Code Lengths Via Serial Commands** on page B-8.

- **One Discrete Length** - Select this option to decode only those codes containing a selected length. For example, select **MSI Plessey - One Discrete Length**, then scan **1, 4** to limit the decoding to only MSI Plessey symbols containing 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



MSI - One Discrete Length

- **Two Discrete Lengths** - Select this option to decode only those codes containing two selected lengths. For example, select **MSI Plessey - Two Discrete Lengths**, then scan **0, 6, 1, 4** to decode only MSI Plessey symbols containing 6 or 14 characters. Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



MSI - Two Discrete Lengths

- **Length Within Range** - Select this option to decode codes within a specified range. For example, to decode MSI symbols containing between 4 and 12 characters, first scan **MSI Plessey - Length Within Range**. Then scan **0, 4, 1** and **2** (single digit numbers must always be preceded by a leading zero). Numeric bar codes begin on page 8-71. To change the selection or cancel an incorrect entry, scan **Cancel** on page 8-72.



MSI - Length Within Range

- **Any Length** - Scan this option to decode MSI Plessey symbols containing any number of characters.



Note

Selecting this option may lead to misdecodes for MSI codes.

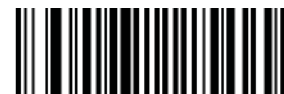


MSI - Any Length

1.5.67 MSI Check Digits

Parameter # 0x32

These check digits at the end of the bar code verify the integrity of the data. At least one check digit is always required. Check digits are not automatically transmitted with the data.



*One MSI Check Digit
(0x00)

If two check digits is selected, also select an MSI Check Digit Algorithm. See page 8-56.



Two MSI Check Digit
(0x01)

RSS

1.5.68 Transmit MSI Check Digit

Parameter # 0x2E

Scan this symbol to transmit the check digit with the data.



**Transmit MSI Check Digit (Enable)
(0x01)**

Scan this symbol to transmit data without the check digit.



***Do Not Transmit MSI Check Digit (Disable)
(0x00)**

1.5.69 MSI Check Digit Algorithm

Parameter # 0x33

When the Two MSI check digits option is selected, an additional verification is required to ensure integrity. Select one of the following algorithms.



**MOD 10/ MOD 11
(0x00)**



***MOD 10/ MOD 10
(0x01)**

1.5.70 Enable/Disable RSS-14

Parameter # 0xF0 0x52

To enable or disable RSS-14, scan the appropriate bar code below.



**Enable RSS-14
(0x01)**



***Disable RSS-14
(0x00)**

1.5.71 Enable/Disable RSS-Limited

Parameter # 0xF0 0x53

To enable or disable RSS-Limited, scan the appropriate bar code below.



**Enable RSS-Limited
(0x01)**



***Disable RSS-Limited
(0x00)**

1.5.72 Enable/Disable RSS-Expanded

Parameter # 0xF0 0x54

To enable or disable RSS-Expanded, scan the appropriate bar code below.



**Enable RSS-Expanded
(0x01)**



***Disable RSS-Expanded
(0x00)**

1.5.73 Transmit Code ID Character

Parameter # 0x2D

A code ID character identifies the code type of a scanned bar code. This can be useful when decoding more than one code type. The code ID character is inserted between the prefix character (if selected) and the decoded symbol.

Select no code ID character, a Symbol Code ID character, or an AIM Code ID character. The Symbol Code ID characters are listed below; see B for **AIM Code Identifiers**.

- A = UPC-A, UPC-E, UPC-E1, EAN-8, EAN-13
- B = Code 39, Code 32
- C = Codabar
- D = Code 128, ISBT 128
- E = Code 93
- F = Interleaved 2 of 5
- G = Discrete 2 of 5
- J = MSI
- K = UCC/EAN-128
- L = Bookland EAN
- M = Trioptic Code 39
- N = Coupon Code
- R = RSS-14, RSS-Limited, RSS-Expanded



**Symbol Code ID Character
(0x02)**



**Aim Code ID Character
(0x01)**



***None
(0x00)**

1.5.74 Prefix/Suffix Values

Parameter # P = 0x69, S1 = 0x68, S2 = 0x6A

A prefix and/or one or two suffixes can be appended to scan data for use in data editing. To set these values, scan a four-digit number (i.e. four bar codes) that corresponds to ASCII values. See the Table B-5 on page B-9, and **Numeric Bar Codes** on page 8-71. To change the selection or cancel an incorrect entry, scan the Cancel bar code on page 8-72. To set the Prefix/Suffix values via serial commands, see Setting Prefixes and Suffixes Via Serial Commands on page B-9.



In order to use Prefix/Suffix values, the Scan Data Transmission Format must be set. See page 8-61.



Scan Prefix



Scan Suffix 1



Scan Suffix 2



Data Format Cancel

Serial Parameters

1.5.75 Scan Data Transmission Format

Parameter # 0xEB

To change the Scan Data Transmission Format, scan one of the eight bar codes corresponding to the desired format.



***Data As Is
(0x00)**



**<DATA> <SUFFIX 1>
(0x01)**



**<DATA> <SUFFIX 2>
(0x02)**



**<DATA> <SUFFIX 1> <SUFFIX 2>
(0x03)**



**<PREFIX> <DATA>
(0x04)**



**<PREFIX> <DATA> <SUFFIX 1>
(0x05)**



**<PREFIX> <DATA> <SUFFIX 2>
(0x06)**



**<PREFIX> <DATA> <SUFFIX 1> <SUFFIX 2>
(0x07)**

1.5.76 Baud Rate

Parameter # 0x9C

Baud rate is the number of bits of data transmitted per second. The scanner's baud rate setting should match the data rate setting of the host device. If not, data may not reach the host device or may reach it in distorted form.



**Baud Rate 300
(0x01)**



**Baud Rate 600
(0x02)**



**Baud Rate 1200
(0x03)**



**Baud Rate 2400
(0x04)**



**Baud Rate 4800
(0x05)**



***Baud Rate 9600
(0x06)**



**Baud Rate 19,200
(0x07)**



**Baud Rate 38,400
(0x08)**

1.5.77 Parity

Parameter # 0x9E

A parity check bit is the most significant bit of each ASCII coded character. Select the parity type according to host device requirements.

If you select **ODD** parity, the parity bit has a value 0 or 1, based on data, to ensure than an odd number of 1 bits is contained in the coded character.



**Odd
(0x00)**

If you select **EVEN** parity, the parity bit has a value 0 or 1, based on data, to ensure than an even number of 1 bits is contained in the coded character.



**Even
(0x01)**

Select **MARK** parity and the parity bit is always 1.



**Mark
(0x02)**

Select **SPACE** parity and the parity bit is always 0.



**Space
(0x03)**

If no parity is required, select **NONE**.



***None
(0x04)**

1.5.78 Software Handshaking

Parameter # 0x9F

This parameter offers control of the data transmission process in addition to that offered by hardware handshaking. Hardware handshaking is always enabled and cannot be disabled by the user.

Disable ACK/NAK Handshaking

When this option is selected, the decoder will neither generate nor expect ACK/NAK handshaking packets.



**Disable ACK/NAK
(0x00)**

Enable ACK/NAK Handshaking

When this option is selected, after transmitting data, the scanner expects either an ACK or NAK response from the host. The scanner also ACKs or NAKs messages from the host.

The scanner waits up to the programmable Host Serial Response Time-out to receive an ACK or NAK. If the scanner does not get a response in this time, it resends its data up to two times before discarding the data and declaring a transmit error.



***Enable ACK/NAK
(0x01)**

1.5.79 Decode Data Packet Format

Parameter # 0xEE

This parameter selects whether decoded data is transmitted in raw format (unpacked), or transmitted with the packet format as defined by the serial protocol. If the raw format is selected, ACK/NAK handshaking is disabled for decode data.



***Send Raw Decode Data
(0x00)**



**Send Packeted Decode Data
(0x01)**

1.5.80 Host Serial Response Time-out

Parameter # 0x9B

This parameter specifies how long the decoder waits for an ACK or NAK before resending. Also, if the decoder wants to send, and the host has already been granted permission to send, the decoder waits for the designated time-out before declaring an error.

The delay period can range from 0.0 to 9.9 seconds in 0.1 second increments. After scanning the bar code below, scan two numeric bar codes beginning on page 8-71. Values less than 10 require a leading zero. To change the selection or cancel an incorrect entry, scan the **Cancel** bar code on page 8-72.



Host Serial Response Time-out
(Default: 2.0 sec.)

1.5.81 Stop Bit Select

Parameter # 0x9D

The stop bit(s) at the end of each transmitted character marks the end of transmission of one character and prepares the receiving device for the next character in the serial data stream. Set the number of stop bits (one or two) to match host device requirements.



***1 Stop Bit**
(0x01)



2 Stop Bits
(0x02)

1.5.82 Intercharacter Delay

Parameter # 0x6E

The intercharacter delay gives the host system time to service its receiver and perform other tasks between characters. Select the intercharacter delay option matching host requirements. The delay period can range from no delay to 99 msec in 1 msec increments. After scanning the bar code below, scan two bar codes beginning on page 8-71 to set the desired time-out. To change the selection or cancel an incorrect entry, scan the **Cancel** bar code on page 8-72.



Intercharacter Delay
(Default: 0 sec.)

1.5.83 Host Character Time-out

Parameter # 0xEF

This parameter determines the maximum time the decoder waits between characters transmitted by the host before discarding the received data and declaring an error. The time-out is set in 0.01 second increments from 0.01 seconds to 0.99 seconds. After scanning the bar code below, scan two bar codes beginning on page 8-71 to set the desired time-out. To change the selection or cancel an incorrect entry, scan the **Cancel** bar code on page 8-72.



Host Character Time-out
(Default: 200 msec.)

Event Reporting

The host can request the decoder to furnish certain information (events) relative to the decoder's behavior. Enable or disable the events listed in Table 8-2 by scanning the appropriate bar codes on the following pages. Parameter number format for these parameters follows those shown in Table 9-9 on page 9-20 for parameters numbered 256 or higher.

Event Class	Event	Code Reported
Decode Event	Non parameter decode	0x01
Boot Up Event	System power-up	0x03
Parameter Event	Parameter entry error	0x07
	Parameter stored	0x08
	Defaults set (and parameter event is enabled by default)	0x0A
	Number expected	0x0F

1.5.86 Parameter Event

Parameter # 0xF0 0x03

When enabled, the decoder sends a message to the host when one of the events specified in Table 8.2 on page 8-69 occurs. When disabled, no message is sent.



**Enable
(0x01)**



***Disable
(0x00)**

1.5.84 Decode Event

Parameter # 0xF0 0x00

When enabled, the decoder generates a message to the host whenever a bar code is successfully decoded. When disabled, no notification is sent.



**Enable
(0x01)**



***Disable
(0x00)**

1.5.85 Boot Up Event

Parameter # 0xF0 0x02

When enabled, the decoder sends a message to the host whenever power is applied. When disabled, no message is sent.



**Enable
(0x01)**



***Disable
(0x00)**

Numeric Bar Codes

For parameters requiring specific numeric values, scan the appropriately numbered bar code(s).



0



1



2



3



4



5



6



7



8



9

1.5.87 Cancel

To change the selection or cancel an incorrect entry, scan the bar code below.

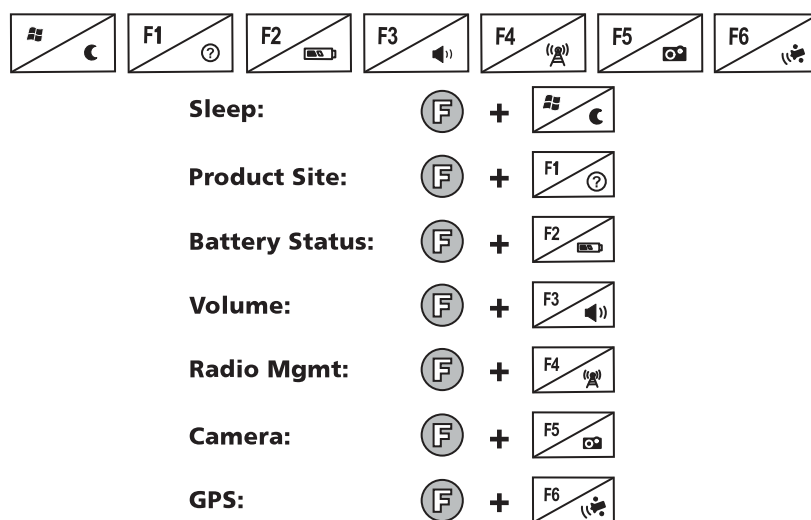


Cancel

1.4 Using the Function Button

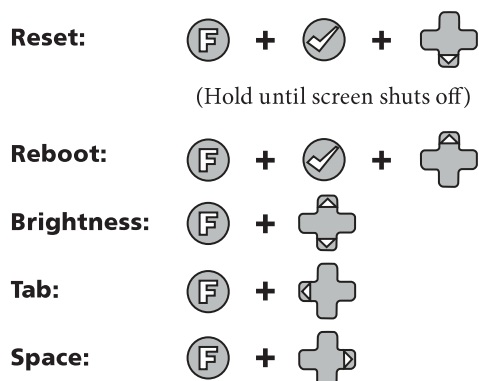
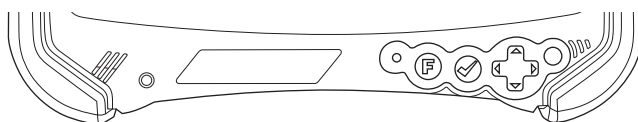
1.1.1 Using the Function Button With the Function Keys

Each Function Key has two states. The first is its programmable function. The second is indicated by an icon representing its function and is activated as shown below:



1.1.1 Using the Function Button Combinations

This unit provides certain commands through function button combinations. The combinations listed below provide access to the specific options listed below:



2.0 Summit Radio

2.1 Summit Client Utility

To launch, go to:

Start > Programs > Summit > Summit Client Utility

2.1.1 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).

The following images (in Figure 1) are the SCU Main windows for Windows CE/Windows Mobile:

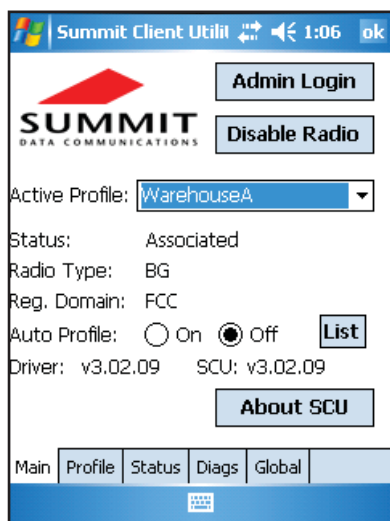


Figure 1 — Main Window

2.1.1.1 Main Window Elements

Table 1 describes the SCU elements available from the Main window:

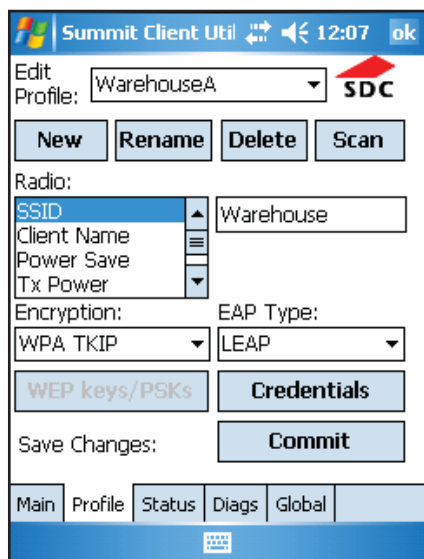
Element	Description										
Admin Login/Logout	Administrator use only.										
Enable Radio /Disable Radio	When the radio is enabled, select this button (which displays Disable Radio) to disable it. When the radio is disabled, select the same button (which now displays Enable Radio) to enable it. Note: When the radio is enabled, it attempts to make and/or maintains a connection to an access point. When a radio is disabled, its power remains on but it does not attempt to make a connection to an access point.										
Status	Indicates the current status of the Summit radio. Connection status options include: <table border="1"> <tr> <td>Down</td><td>The radio is not recognized by Summit software and therefore is not associated nor authenticated.</td></tr> <tr> <td>Disabled</td><td>The radio is disabled. To enable the radio, tap Enable Radio located on the SCU Main window. When the radio is disabled, it does not attempt to make a connection to an access point.</td></tr> <tr> <td>Not Associated</td><td>The radio has not established a connection to an access point.</td></tr> <tr> <td>Associated</td><td>The radio has established a connection to an access point but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.</td></tr> <tr> <td><EAP type> Authenticated</td><td>The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).</td></tr> </table>	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 window. 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 but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.	<EAP type> Authenticated	The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).
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 window. 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 but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.										
<EAP type> Authenticated	The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).										
Radio Type	Indicates the type of radio installed in the device. For example: <table border="1"> <tr> <td>BG</td><td>Indicates a Summit 802.11g radio which supports 802.11b and 802.11g.</td></tr> <tr> <td>ABG</td><td>Indicates a Summit 802.11a/g radio which supports 802.11a, 802.11b, and 802.11g.</td></tr> <tr> <td>N</td><td>Indicates Summit 802.11n radio which supports 802.11a, 802.11b, 802.11g, and 802.11n.</td></tr> </table>	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 Summit 802.11n radio which supports 802.11a, 802.11b, 802.11g, and 802.11n.				
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 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.										
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: There is a limit of 19 profiles in the Auto Profile list. Note: Auto Profile is only available on Windows CE and Windows Mobile operating systems.										
Driver	Indicates the current version of the device driver.										
SCU	Indicates the SCU version currently running on the device. Displays only if space permits.										

Table 1 — Main Window Elements

2.1.2 Profile Window

Profile settings are radio and security settings that are stored for each configuration profile. Other than viewing the settings for each profile, the functions and settings located on the Profile window are only available to administrators. Non-administrators may not edit any items on this tab.

The following two images (in Figure 2) are the SCU Profile windows for Windows CE and Windows XP operating systems:

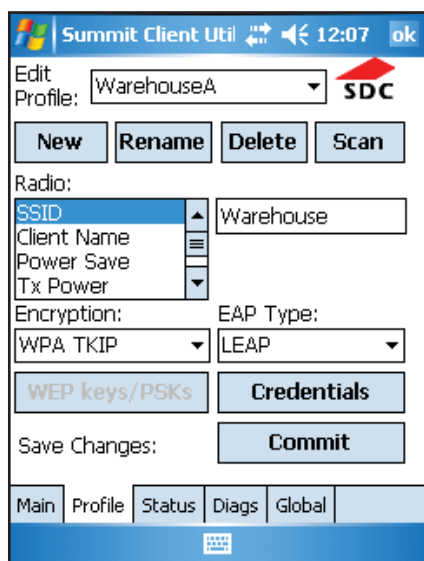


Note: The Summit Glossary of Technical Terms provides detailed information for the following radio setting terms located on the Profile tab. Refer to the Administrator's Guide for SCU-specific radio settings including default settings.

2.1.3 Status Window

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

The following image is the SCU Status window for Windows CE operating system:



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).

Element	Description										
Profile	The active profile.										
Status	Indicates the current status of the Summit radio. Status also displays on the Main tab window. See Main Window > Status for details on individual status options. Connection status options include: <table border="1"> <tr> <td>Down</td><td>The radio is not recognized by Summit software and therefore is not associated nor authenticated.</td></tr> <tr> <td>Disabled</td><td>The radio is disabled. To enable the radio, tap Enable Radio located on the SCU Main window. When the radio is disabled, it does not attempt to make a connection to an access point.</td></tr> <tr> <td>Not Associated</td><td>The radio has not established a connection to an access point.</td></tr> <tr> <td>Associated</td><td>The radio has established a connection to an access point but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.</td></tr> <tr> <td><EAP type> Authenticated</td><td>The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).</td></tr> </table>	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 window. 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 but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.	<EAP type> Authenticated	The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).
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 window. 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 but is not EAP authenticated. The radio can not communicate unless it is associated and EAP authenticated. Note: If the Encryption type is set to WEP or Open (None), it can communicate (send data) while in the Associated state.										
<EAP type> Authenticated	The radio has established a connection to an access point and has completed EAP authentication successfully. In this state, the radio can communicate (send data).										
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 Tx Power. This section also displays the signal strength (or RSSI) in dBm and quality. Note: For more information on 802.11 channels, refer to the Summit Glossary of Technical Terms.										

Table 2 — Status Window Elements

2.1.4 Diags Window

The Status window provides status information on the radio connection between the client device and the access point to which it's associated. The following image is the SCU Status window for Windows CE operating system:

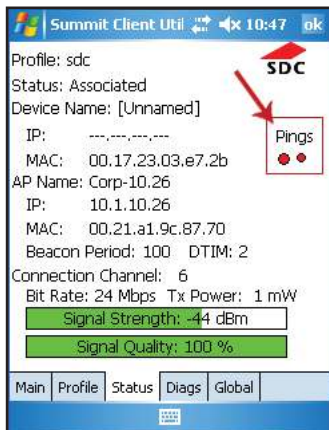


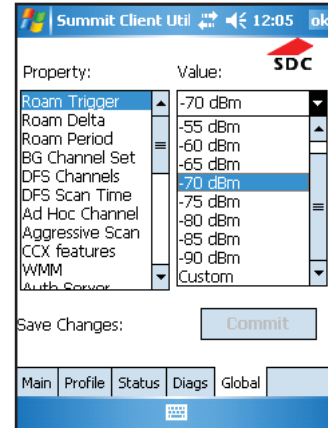
Table 3 below describes the SCU elements available from the Diags window.

Element	Description
(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 Summit radio and another network adapter active, then pings may go out over the non-Summit 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 (re)connect 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 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).

Table 3 — Diags Window Elements

2.1.5 Global Window

Global settings include radio and security settings that apply to all profiles and settings that apply to SCU itself. Administrator use only. The following image is the SCU Global window for Windows CE operating system.






Detailed definitions of all properties located on the Global window can be found in the Summit Glossary of Technical Terms:



Terms	Definitions
Ad Hoc Channel	Ad Hoc Channel is an 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. Ad Hoc Channel options include: <ul style="list-style-type: none"> One of the 2.4 GHz channels (1-14) One of the UNII-1 channels (36, 40, 44, 48) Note: If you select a channel that is not supported by your radio, then SCU uses the default channel setting (1) for this setting.
Admin Passwords (Admin Only)	
Aggressive Scan	Aggressive Scan is an SCU Global setting. 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 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 access points that are on the same channel.
Auth Server	Auth Server is an SCU Global setting that indicates the type of authentication server being used for EAP. Auth Server options include: <ul style="list-style-type: none"> Type 1 - Cisco Secure ACS or another server that uses PEAPv1 for PEAP with EAP-MSCHAPV2 (PEAP-MSCHAP). Type 2 - A different authentication server, such as Juniper Networks Steel Belted RADIUS, that uses PEAPv0 for PEAP-MSCHAP.

Auth Time-outs	<p>Auth Timeout is an SCU Global setting that specifies the number of seconds (from 3 to 60) that Summit 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.</p> <p>The default Auth Timeout value is 8 seconds</p>
BG Channel Set	<p>BG Channel Set is an SCU Global setting that 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:</p> <ul style="list-style-type: none"> • 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 these three channels which are most commonly used in ETSI and TELEC. • 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. <ul style="list-style-type: none"> – If the registry is edited but the user does not select Custom, SCU ignores the registry. – If SCU displays a value other than Custom and the user selects Custom, SCU reverts to the value that it displayed before the user selected Custom.
CCX features	<p>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. CCX Features options are:</p> <ul style="list-style-type: none"> • 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. <p>Note: For Summit 30AG (SDC-MSD30AG and SDC-SSD30AG) radio modules, this parameter is disabled. The default is Optimized.</p>
Certs Path	<p>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.</p> <p>The SCU default certification path depends on the type of device.</p>

DFS Channels	<p>DFS Channels is an SCU Global setting that 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. DFS Channels options include:</p> <ul style="list-style-type: none"> • 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). <p>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.</p> <p>Note: The Optimized setting is not supported in the MSD30AG and SSD30AG radios. If DFS Channels is set to Optimized directly in the registry, the setting will function as On (versus Optimized).</p>
DFS Scan Time	<p>Because passive scanning consumes a longer period of time, DFS Scan Time (an SCU Global setting) enables you to determine the dwell (listen) time (in milliseconds or ms) when passively scanning on a DFS channel.</p> <p>Note: 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, Summit 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 ms, the beacon period should be adjusted to 20 ms.</p> <p>Note: If you adjust this parameter directly in the registry, and configure it to a number outside of the 20-500 ms range, the setting value will return to the default (120 ms).</p>
Frag Thresh	<p>Frag Thresh (fragmentation threshold) is an SCU Global setting that indicates the packet size (in bytes) at which the packet is fragmented. For SCU, the Frag Thresh integer range is 256 to 2346 (bytes) with a default setting of 2346 bytes.</p> <p>Note: For 30AG (SDC-MSD30AG and SDC-SSD30AG) radio modules, this parameter is disabled.</p>
Hide Passwords	<p>Hide Passwords is an SCU Global setting that indicates whether or not security information is masked. If this setting is turned on, SCU (along with EAP authentication dialog boxes) masks credentials and other sensitive information.</p> <p>The SCU default setting is Off.</p>
LED	<p>LED is an SCU Global setting that indicates whether or not an LED is used. This setting applies only to select Summit devices/radios.</p>
Logon Options	

Ping Delay ms	<p>Ping Delay is an SCU Global setting that indicates the amount of time (in milliseconds or ms) between successive ping requests.</p> <p>A ping timeout integer value can range from 0 to 7200000 ms. The SCU default is 1000 ms.</p>
Ping Payload	<p>Ping Payload is an SCU Global setting that indicates the amount of data (in bytes) that is transmitted on a ping.</p> <p>Ping payload values include 32, 64, 128, 256, 512, and 1024 bytes. The SCU default is 32 bytes.</p>
Ping Timeout ms	<p>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.</p> <p>A ping timeout integer value can range from 1 to 30000 ms. The SCU default is 5000 ms.</p>
PMK Caching	<p>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.</p> <p>PMK caching is an alternative to CCKM supported with WPA2. The goal of PMK caching is to speed up roaming between access points by accomplishing 802.1X reauthentications without communicating with the authentication server. When a station does an initial authentication to the WLAN infrastructure, both sides receive the information needed for reauthentications.</p> <p>If there are no controllers, then Standard PMK caching is used and reauthentication information is cached only on the initial access point. When the station tries to reauthenticate to that access point, the station and the access point use the cached information to do the four-way handshake to exchange keys.</p> <p>If there are controllers, then Opportunistic PMK (OPMK) caching is used and reauthentication information is cached on the controllers. When the station tries to reauthenticate, the station and the controller behind the access point use the cached information to do the four-way handshake to exchange keys.</p> <p>Use the PMK Caching global setting to configure the type of PMK caching supported by your infrastructure. If the Summit radio is configured for one type of PMK caching and the infrastructure supports the other type, then PMK caching will not work, and every roam will require a full 802.1X authentication that requires interaction with an authentication server.</p> <p>If the active profile has an Encryption setting of WPA2 CCKM, then the Summit radio ignores the PMK Caching global setting and attempts to use CCKM.</p>
Roam Delta	<p>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.</p> <p>Note: For an example of how Roam Delta works, refer to Standard Roaming.</p>
Roam Period	<p>Roam period indicates the amount of time a radio collects RSSI scan data (after association or a roam scan) before it considers roaming to a different access point.</p> <p>Note: For an example of how Roam Period works, refer to Standard Roaming.</p>

Roam Trigger	<p>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.</p> <p>Note: For an example of how Roam Trigger works, refer to Standard Roaming.</p>
RTS Thresh	<p>RTS Thresh (Request To Send threshold) is an SCU Global setting that indicates the packet size (in bytes) at which a Request To Send (RTS) or Clear To Send (CTS) is required on the link.</p> <p>For SCU, the RTS Thresh integer range is 0 to 2347 (bytes) with a default setting of 2347 bytes.</p> <p>Note: For 30AG (MSD30AG and SSD30AG) radio modules, this parameter is disabled.</p>
Rx Diversity	<p>Antenna diversity refers to the use of multiple antennas to increase the odds that a functional signal is received.</p> <p>Rx (Receive) Diversity is an SCU Global setting that indicates how to handle antenna diversity when receiving data from an access point. Rx Diversity setting options include:</p> <ul style="list-style-type: none"> 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. <p>Note: Summit does not support the AUX antenna as a single-antenna solution.</p>
Tray Icon	<p>Tray Icon is an SCU Global setting that allows you to enable or disable the System Tray icon.</p> <p>The tray icon provides a visual status for the device's Summit radio and it enables the user to launch SCU. This service is available only for Windows CE and Windows Mobile.</p> <p>The software for the service is installed with other Summit software in a .cab file. The service is active only when all of the following are true:</p> <ul style="list-style-type: none"> 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 <p>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:</p> <p> The radio is not associated/authenticated to an access point.</p> <p> 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.</p> <p> 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.</p> <p>(cont'd)</p>

Tray Icon (cont'd)	 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.
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. Inner authentication methods include: <ul style="list-style-type: none"> • Auto-EAP - Any available EAP method • MSCHAP • MSCHAPV2 • PAP • CHAP • EAP-MSCHAPV2 - See MSCHAPV2. The SCU TTLS Inner Method default setting is Auto-EAP.
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. Tx Diversity setting options include: <ul style="list-style-type: none"> • Main only - Indicates use of the main antenna only. • Aux only - Indicates use of the auxiliary antenna only. Note: Summit does not support the AUX antenna as a single-antenna solution. <ul style="list-style-type: none"> • On - Indicates the use of diversity (both antennas).
WMM	WMM (Wi-Fi Multimedia) extensions for WLANs allow the prioritization of voice traffic. WMM is a subset of 802.11e. WMM is an SCU Global setting that enables or disables the use of WMM extensions. 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.

2.1.6 Using the Summit System Tray Icon

Summit software includes a service that displays an icon in the Windows System Tray. This icon provides a visual status for the Summit radio in the device and it provides access to the SCU application.



Note: Tap the icon to launch the SCU application.

The service is active and displays an icon in the System Tray only when all of the following conditions are met:

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

When the service is active, it queries the radio every three seconds for connection status. Based on the radio's response to the query, the service 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.

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

Appendix A — EAP Types

AES	<p>AES-CCMP is the encryption method defined with IEEE 802.11i and certified with WPA2. Stronger than RC4 (which is used with both WEP and TKIP), AES-CCMP is considered sufficient for FIPS 140-2.</p> <p>AES - Advanced Encryption Standard CCMP - Counter Mode CBC-MAC Protocol</p>
Authentication	<p>The process of verifying the identity of:</p> <ul style="list-style-type: none"> A station attempting to gain access to a network. A network to which a station is trying to gain access. <p>IEEE 802.1X, which is the authentication component of WPA and WPA2, performs mutual authentication through an Extensible Authentication Protocol (EAP) type. With mutual authentication, the network authenticates the station and the station authenticates the network.</p>
Auth Type	<p>Auth Type indicates the 802.11 authentication type used when associating to an access point. SCU authentication type parameters include:</p> <ul style="list-style-type: none"> Open - This two-step authentication type involves the station sending a request (usually a randomly generated key) to the access point. The access point sends an authentication response that contains a success or failure message. Once accepted, the key is only used for a short period of time; then a new key is generated and agreed upon. Shared (Shared-key) - With a shared authentication type, both the station and the access point have the same "shared" key or passphrase. LEAP (Network-EAP) <p>Note: See http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801bd035.shtml for a Cisco explanation of 802.11 authentication using Open and Network-EAP. The Summit Client Utility refers to Network-EAP as LEAP.</p> <p>Note: Summit highly recommends the use of Open which is also the SCU default. This setting can be edited from the Profile window of SCU.</p>
Bit Rate	<p>Bitrate is the measurement of how much data is transmitted in a given amount of time from one location to another. It is generally measured in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).</p>
CAM	<p>CAM (Constantly Awake Mode) is a power save mode that keeps the radio powered up continuously to ensure there is minimal lag in response time. This power save setting consumes the most power but offers the highest throughput.</p>
CKIP	<p>CKIP (Cisco Key Integrity Protocol) and CMIC (Cisco Message Integrity Check) are Cisco-defined predecessors to WPA TKIP and are supported only on Cisco Wi-Fi infrastructure. An SCU profile setting of CKIP (not CKIP-EAP) means that the encryption keys are defined in SCU. An SCU profile setting of CKIP-EAP means that the encryption keys are derived dynamically from an EAP authentication.</p> <p>Note: If the SCU active profile has an encryption setting of CKIP or CKIP EAP, then the Summit radio associates or roams successfully to an access point that is configured with the following: (cont'd)</p>

CKIP (cont'd)	<ul style="list-style-type: none"> The SSID and other RF settings of the SCU active profile The authentication method of the SCU active profile Any of the following encryption settings: <ul style="list-style-type: none"> WEP only (no CKIP or CMIC) WEP with CKIP WEP with CMIC WEP with CKIP and CMIC <p>Note: Summit recommends the use of TKIP or WPA2.</p>
Client Name	<p>For the SCU, the device name assigned to the Summit radio and the client device that uses it.</p> <p>Note: If CCX Features are set on the SCU Global settings page, then the client name is relayed and used for association.</p>
Credentials	<p>The Credentials button on the Profile window of SCU allows you to add or edit the authentication credentials for the selected EAP type. See Table X — EAP Credentials for more information.</p>
EAP	<p>See Table X — EAP Credentials</p>
Fast	<p>Fast is a power save mode that switches between PSP (Power Save Protocol) mode and CAM mode, depending on network traffic. For example, it switches to CAM when it is receiving a large number of packets and switches back to PSP after the packets have been retrieved. Fast is recommended when power consumption and throughput is a concern.</p>
Encryption	<p>Encryption involves scrambling transmitted data so that it can be read only by the intended receiver, which has the proper key to decrypt unscramble the encrypted data. In Summit Client Utility, the Encryption setting in a profile can refer not just to an encryption method but also to an authentication method and an encryption key management protocol.</p> <p>For more information, see "SCU Encryption Settings" Table.</p>
Maximum	<p>Maximum (Max PSP) is a power save mode where the access point buffers incoming messages for the radio. The radio occasionally 'wakes up' to determine if any buffered messages are waiting and then returns to sleep mode after it requests each message. This setting conserves the most power but also provides the lowest throughput. It is recommended for radios in which power consumption is most important (such as small battery-operated devices).</p>
Power Save	<p>Indicates the radio's current power save setting. Power save mode allows you to set the radio to its optimum power-consumption setting.</p> <p>Maximizing battery life for full shift operation is an important consideration for vendors and users of hand-held data terminals and similar devices. Summit provides a number power save modes that can significantly reduce the radio's power consumption and maximize the battery life of the host device.</p> <p>(cont'd)</p>

Power Save (cont'd)	<p>Summit supports the three following power save modes:</p> <ul style="list-style-type: none"> • CAM (Constantly Awake Mode) • Fast • Maximum <p>When in power save mode, the radio “sleeps” most of the time and “wakes up” only when it has data that needs to be sent to the infrastructure (or at an interval determined between the station and the access point). When the radio is awake, the access point also delivers to the station any data that has been buffered during the radio’s sleep period.</p>
Radio Mode	<p>Radio mode is an 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 station radio instead of an access point.</p> <p>When SCU operates with a Summit 802.11g radio, an administrator can select from among the following radio mode values:</p> <ul style="list-style-type: none"> • 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, Summit recommends BG rates full. • Ad Hoc - When selected, the Summit 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 station radio that is in ad hoc mode and has the same SSID and, if configured, static WEP key. <p>Note: The default is BG rates full.</p> <p>Note: See “802.11a/g Radio Mode with 802.11g Radio” for additional information.</p> <p>When SCU operates with a Summit 802.11a/g radio, an administrator can select from the following radio mode values:</p> <ul style="list-style-type: none"> • 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 (see “Preferred Band for 802.11a/g Radio” for more information). • BGA rates full - All B and G rates and all A rates, with B and G rates (the .11g radio) preferred (see “Preferred Band for 802.11a/g Radio” for more information). • 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, Summit recommends BG rates full. <p style="text-align: right;">(cont'd)</p>

Radio Mode (cont'd)	<ul style="list-style-type: none"> • Ad Hoc - When selected, the Summit 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 station radio that is in ad hoc mode and has the same SSID and, if configured, static WEP key. <p>Note: The default is ABG rates full.</p> <p>Note: See “802.11a/g Radio Mode with 802.11g Radio” for additional information.</p> <p>Preferred Band for 802.11a/g Radio</p> <p>When the radio mode value is ABG rates full, the 5 GHz (A) band is preferred over the 2.4 GHz (BG) band. When the radio mode value is BGA rates full, the 2.4 GHz (BG) band is preferred over the 5 GHz (A) band.</p> <p>When trying to associate to an access point, the radio considers access points in the preferred band. If the radio is able to associate to one of these access points, then the radio will not try to associate to an access point in the other band. The only time that the radio attempts to associate to an access point in the non-preferred band is when the radio is not associated and cannot associate in the preferred band.</p> <p>When roaming, the radio considers only access points in the current band (the band in which the radio is currently associated). The radio will consider an access point in the other band only if it loses association.</p> <p>802.11a/g Radio Mode with 802.11g Radio</p> <p>When an administrator tries to create or edit a profile, SCU determines which radio is operating in the device and populates the available radio mode values according to the radio type. Suppose a profile created for an 802.11a/g card is loaded on a device with an 802.11g card. If a radio mode value of A rates only, ABG rates full, or BGA rates full was set in the profile, then SCU displays a value of BG rates full. If the administrator does not save any changes to the profile, then SCU leaves the profile, including the radio mode, unchanged. If the administrator saves any changes to the profile, then SCU saves the radio mode value as BG rates full.</p>
SSID	<p>Service Set Identifier. Unique name of up to 32 characters that identifies a particular 802.11 WLAN.</p> <p>The SSID is attached to the header of packets that are sent over a wireless network.</p>
Tx Power	<p>In SCU, Tx Power displays on the Status window to indicate of the power of the radio, in milliwatts (mW). This value can be overwritten by the AP; the AP can dictate to the client what power to use.</p>
WEP	<p>WEP (Wired Equivalent Privacy) encrypts transmitted data using 64-bit or 128-bit encryption. WEP, which was defined with the original IEEE 802.11 standards, is not recommended because a WEP key can be “broken” in less than an hour using commonly available tools.</p>

WPA/WPA2	<p>WPA (Wi-Fi Protected Access) and WPA2 (Wi-Fi Protected Access 2) are security certifications defined by the Wi-Fi Alliance. To earn a WPA or WPA2 certification, a product must pass a set of tests that elements of the security specification have been implemented correctly. Since March 2006, WPA2 is mandatory for all new equipment that is certified by the Wi-Fi Alliance.</p> <p>Both WPA and WPA2 include three security elements: authentication, encryption, and encryption key management. WPA and WPA2 support the same authentication methods and similar key management methods. The primary difference between the two is in the area of encryption: WPA defines TKIP as the primary encryption method; WPA2 defines AES-CCMP as the primary encryption method.</p> <p>Both WPA and WPA2 include a Personal version and an Enterprise version. With WPA-Personal and WPA2-Personal, which SCU refers to as WPA-PSK and WPA2-PSK, authentication is done through a pre-shared key (PSK) or passphrase that is statically configured on every client device and infrastructure device. With WPA-Enterprise and WPA2-Enterprise, authentication is IEEE 802.1X, which uses an EAP type. WPA2-Enterprise is the equivalent of IEEE 802.11i, the ratified standard for Wi-Fi security.</p>
-----------------	--

EAP-Type	User	Password	CA Cert	Validate Server	User MS Store	Others
PEAP-MSCHAP	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)	Filename (up to 32 characters) See Note on CA Cert Field	See Note on Validate Server Checkbox	See Note on Use MS store Checkbox	
PEAP-TGC	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)	Filename (up to 32 characters) See Note on CA Cert Field	See Note on Validate Server Checkbox	See Note on Use MS store Checkbox	
PEAP-TLS	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)	Filename (up to 32 characters) See Note on CA Cert Field	See Note on Validate Server Checkbox	See Note on Use MS store Checkbox	
EAP-TTLS	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)	Filename (up to 32 characters) See Note on CA Cert Field	See Note on Validate Server Checkbox	See Note on Use MS store Checkbox	
EAP-TLS	Username or Domain/Username (up to 64 characters)		Filename (up to 32 characters) See Note on CA Cert Field	See Note on Validate Server Checkbox	See Note on Use MS store Checkbox	User Cert See Note on User Cert
EAP-FAST	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)				<ul style="list-style-type: none"> • PAC Filename (up to 32 characters) • PAC Password (up to 32 characters)
LEAP	Username or Domain/Username (up to 64 characters)	Password (up to 32 characters)				

Table X — EAP Credentials

Notes for EAP Credentials

Note on CA Cert Field: This is the filename of the root certificate authority digital certificate. Leave this blank if the Use MS Store checkbox is checked.

Note on 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.

Note: Summit strongly recommends the use of server validation with PEAP-GTC.

Note on 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.

Note on User Cert: Tap the “...” button to select a user (or station) certificate from the Microsoft certificate store. Do not enter a filename; the user certificate must reside in the Microsoft certificate store. When you browse for a certificate, the pop-up box displays Issued By and Issued To.

Of the seven EAP types supported by SCU, all but EAP-FAST and LEAP rely upon information in digital certificates that are created by a certificate authority (CA). To enable a station device to authenticate the server, you must provide a root CA certificate and distribute it to that station. You can store the CA certificate in a device’s Microsoft certificate store or in a specified directory (see Certs Path for additional information regarding a specified directory).

Note: For EAP-TLS, you must also generate a user certificate for each station. The user certificate must be stored in the Microsoft certificate store on the station.

EAP-FAST relies upon strong shared-secret keys that are unique to users (rather than digital certificates). These keys 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 station device in one operation. With manual or out-of-band provisioning, the PAC is created in one step and must then be distributed to the station 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.

Note: If you enter a PAC filename in the SCU field, manual provisioning is used. If you omit the PAC filename, automatic provisioning is used.

EAP-FAST	<i>Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling</i> A protocol that was designed to address the vulnerabilities of LEAP while keeping a “lightweight” implementation. It uses a PAC (Protected Access Credential) to create a TLS tunnel where client credentials are verified.
EAP-TLS	<i>Extensible Authentication Protocol-Transport Layer Security</i> EAP-TLS (created by Microsoft) requires an exchange of proof of identities through public key cryptography (such as digital certificates). EAP-TLS secures this exchange with an encrypted TLS tunnel which helps to resist dictionary or other MitM (Man in the Middle) attacks.
EAP-TTLS	<i>Tunneled Transport Layer Security</i> EAP-TTLS enables WLAN station authentication without requiring the stations to have certificates which creates a simplified architecture of secure WLANs. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.
PEAP	<i>Protected Extensible Authentication Protocol or Protected EAP</i> A protocol that creates an encrypted (and more secure) channel before the password-based authentication occurs.
PEAP-GTC	<i>Generic Token Card</i> An authentication mechanism that allows generic authentication to a number of databases and uses a one-time password (OTP is a password that is only valid for a single login session).
PEAP-MSCHAPv2	<i>Protected EAP-Microsoft Challenge Handshake Authentication Protocol - version 2</i> A protocol designed for a wireless network that is not configured for PKI (public key infrastructure).
PEAP-TLS	<i>Protected Extensible Authentication Protocol-Transport Layer Security</i>
LEAP	<i>Lightweight Extensible Authentication Protocol</i> A proprietary EAP mutual authentication protocol developed by Cisco Systems that uses a username and password system.

Table X — EAP Types

Profile Setting	Authentication	Encryption	Key Management
None	None	None	None
WEP	None	WEP	Static (in SCU)
WEP EAP	EAP Type	WEP	Dynamic (from EAP)
CKIP	None	WEP+CKIP+CMIC	Static (in SCU)
CKIP EAP	EAP Type	WEP+CKIP+CMIC	Dynamic (from EAP)
WPA-PSK	PSK/password (in SCU)	TKIP	WPA
WPA-TKIP	EAP Type	TKIP	WPA
WPA CCKM	EAP Type	TKIP	WPA+CCKM
WPA2-PSK	PSK/password (in SCU)	AES-CCMP	WPA2
WPA2 AES	EAP Type	AES-CCMP	WPA2
WPA2 CCKM	EAP Type	AES-CCMP	WPA2+CCKM

Table X — SCU Encryption Settings

EAP

EAP-FAST

EAP-TLSa

EAP-TTLS

LEAP

PEAP

PEAP-GTC

PEAP-MSCHAP2

PEAP-TLS

PSK

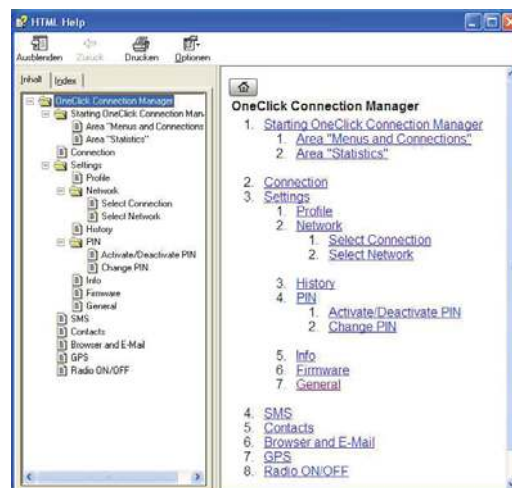
Radio Mode

SSID

Tx Power

WEP

WPA/WPA2



2. Starting the OneClick Connection Manager

OneClick Connection Manager offers everything you need to manage the mobile Internet communication on your Laptop:

- Internet Connection and Email download
- SMS Manager
- Managing contacts from SIM and Outlook
- GPS Management

After installing WebToGo OneClick Internet a new entry will be placed in the program menu. Straight after installation the main window of the application is visible on your screen. If this is not the case you can start the application by going to —

Start -> Programs -> WebToGo OneClick Internet

or click the desktop icon of OneClick Internet.



Whenever the application is active, a status icon will also appear in the toolbar in the bottom right-hand corner of your desktop.

The main window of OneClick Connection Manager is at the heart of the application. Here you can see the status of your OneClick Connection Manager, how much time you have spent on the internet and which data throughput you should expect. You can connect to the internet and send emails or short messages from this window.



The main application is split into two areas:

- Area “Menus and Connection Management”
- Area “Statistics”

Area “Statistics”

This area is split into the following two (2) sub-areas:

Area A

Icon	Description
	Minimize Click this and the OneClick Internet icon will appear in the system tray.
	Close Click this and the application will close.

Area B

Icon	Description
	Indicator of network signal strength, followed by the network name, network mode, and device name.
	Connect — Button to connect or disconnect.
	SMS — Button only enabled if no mobile Internet connection is active. Link to the integrated SMS application.
	Web — Link button to preferred browser.
	Email — Link button to preferred email application.
	GPS — Button to open the GPS tool.
	Radio — Button to switch the radio on and off.
	Statistics — Button to open the Statistics Window.
	Settings — This button opens the Settings Window. It contains: <ul style="list-style-type: none"> • Profile (managing your profiles) • Network (selecting connection and network) • History (data volume transferred) • PIN (PIN settings) • Firmware • Info • General
	Update Database (optional feature) <ul style="list-style-type: none"> • Update database (roaming partner) • Install drivers and new version of OneClick Internet
	Help — Here you can open the Help menu.
Status	Connecting to modem Ready, you can establish connection Connected Failure

Area "Statistics"

Statistics provide advanced information about your connection. All shown data values are approximate values.

Data In:	8.8 KB	Speed:	0 Kbps
Data Out:	8.4 KB	Max. Speed:	0 Kbps
Total:	17.2 KB	Time:	0:00:42

Data In	The amount of data received via the mobile Internet connection.
Data Out:	The amount of data sent via the mobile Internet connection.
Total:	The amount of data sent via the mobile Internet connection.

Speed:	The current speed of the data transfer
Max. Speed	The maximum speed of the data transfer observed.
Time:	The duration of the current connection.

3. Connection Management

1. Launch OneClick Connection Manager and wait until detection has been completed. If you see a detection problem, please reinsert your data card and tap on the connect button. If Pin security is active, a window will pop up asking you to enter your SIM PIN. You can deactivate PIN security in the application if no connection is active: Settings -> PIN -> Deactivate PIN.
2. By default the software comes with no connection profile. You can modify the access details by selecting the "Settings" menu.
3. Now tap on the connect button. That's it.



In the upper status line you can find the indicator for the signal strength, the name of the Mobile Network Operator you are using, a roaming indicator, and the radio technology you are using.

In the status line below the button row you can see the current status of you connection and the device.

4. Settings

To access the Settings menu tap in main window on the button:



A dialog will open showing registers for the following settings:

1. Profile
2. Network
3. History
4. PIN
5. Info
6. Firmware
7. General

Profiles

You are free to create your own connection profile. Once a new profile has been created it will appear in the dropdown menu Profiles. You can select it by tapping on Set Profile to use it.

Button	Description
	Create a new profile
	Edit a current profile
	Delete a profile
	Save a profile
	Set the profile you want to use

Label	Description
Profile Name	Profile name — should be unique
APN	Access Point Name of your network operator. For more details, contact your network operator. When you are registered to a CDMA network, the APN will not appear.
Username	For more details, contact your network operator.
Password	For more details, contact your network operator.
DNS	Domain Name Server — For more details, contact your network operator.
Proxy Settings	Necessary Proxy Settings of your network. For more details, contact your network operator.

Network

You are offered two options: “Select Connection” and “Select Network”.



When you are registered to a CDMA network, you will not be able to select the network. All CDMA network will be shown instead.

Select Connection

Three different settings are available here:

Label	Description
Select automatically	Selects the best suited network available
Only use GPRS	Use only GPRS for a connection
Only use UMTS/HSDPA	Use only UMTS/HSDPA for a connection

Select and tap Register. If the change is successful you will retrieve a message “Network changed successfully”.

Close the window and wait until you see signal strength in the main window. After that you can establish a connection.

Select Network

In this dialog you may select any available network. It is useful when you are abroad.

Automatic mode will select the preferred network of your network operator.

If you select Network selection you will get a list of network options.

1. Automatic Selection
2. Retrieving Networks...

The marked network is the network you’re currently registered with.

NOTE: The network list will only appear if the connection setting is “Only use GPRS” or “Only use UMTS/HSDPA”.

Select the network and tap on the register button. If the change is successful you will see the message “Network changed successfully”.

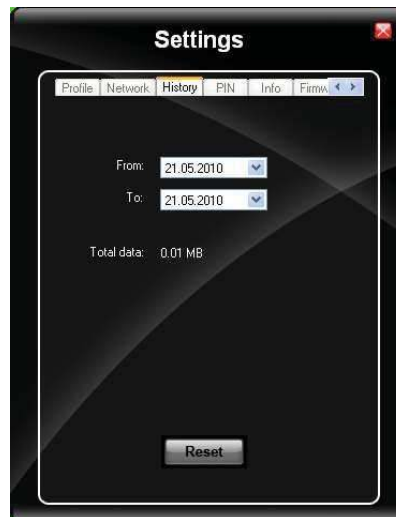
Close this window and wait until you see the signal strength in the main window, then you can establish the connection.

History

The history will show you the data volume transferred in a certain time frame.

Select a time frame to see the data volume sent/received in the selected period.

Tap on “Reset” to reset the counter.



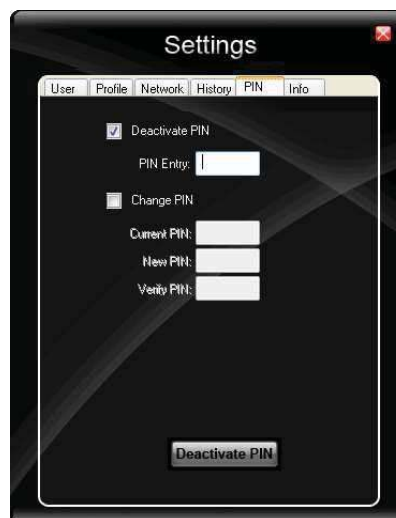
PIN

You can Activate/Deactivate PIN or Change PIN.

1. Activate/Deactivate PIN
2. Change PIN

Activate/Deactivate PIN

Usually you have to enter the PIN each time you start WebToGo One-Click Internet using a modem card. Deactivate the PIN to avoid doing this each time.



Change PIN

This dialog lets you change your PIN.

Label	Description
Current PIN	Enter your current PIN
New PIN	Enter your new PIN
Verify PIN	Enter once again the new PIN

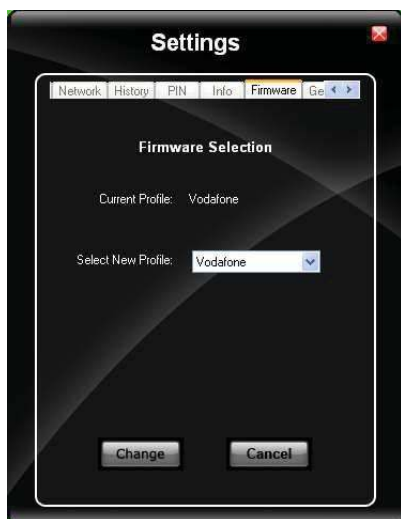
Info

This window shows SIM card, modem and system Information:



Firmware

OneClick Internet will select the correct Firmware matching your operator automatically, if a special firmware for your operator is available and a SIM card is inserted. If no specific firmware for your operator is available, it will select the generic firmware. Once a firmware has been selected, it will appear in "Current Profile".



You are free to load your desired firmware. You can select a new firmware manually by clicking the "Select New Profile" dropdown menu, selecting a firmware from the menu and pressing the "Change" button to load it. If you want to return to automatic firmware selection, please choose "Automatic(UMTS)" in the dropdown menu.

Switching between CDMA and UMTS firmware is not done automatically. You will have to select CDMA firmware manually, if you want to connect to CDMA networks. If you want to return to UMTS networks, you have to manually select UMTS firmware in respect.

Activation on CDMA

When a CDMA Firmware is selected in the Firmware Settings, the activation of the modem on the CDMA network starts automatically. During the process of loading CDMA firmware, an activation window will pop up offering two options: "Manual Activation" and "Automated Activation":

Label	Description
Manual Activation	Speak with a Customer care representative using a standard phone.(Also requires the manual input of certain items). Please enter the activation code, your phone number and the system ID given in the product documentation.
Automatic Activation	Use your modem to start an automated activation session

If you cancel the activation, a dialog will be shown, that gives you the options to select automatic or manual network activation.

When you have cancelled the activation or if it failed before, you can also start the activation manually by pressing the "Activate" button in the "General" tab.



General

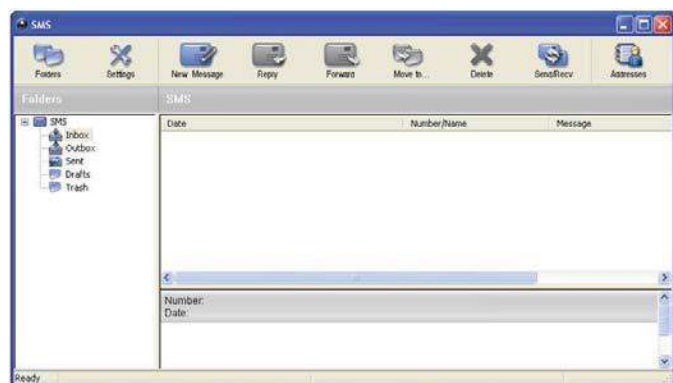
In General settings you can set options to connect automatically and for roaming:












Label	Description
Auto Launch	If selected, OneClick Internet will launch automatically when the user starts up the operating system and logs in.
Connect Automatically	If selected, OneClick Internet will connect automatically on start-up.
Reconnect Automatically	If selected, OneClick Internet will reconnect automatically after standby and hibernate.
Allow roaming	If disabled, OneClick Internet will not allow connections in foreign networks. This feature avoids high costs when roaming.
Roaming Alert	If selected, a dialog will inform you when you are moving from your home network to a roaming network when connected.

5. Application Buttons

SMS



The SMS Center window is split into menu bar, folder view, folder content and preview window. To manage your short messages you may:

Label	Description
 Folders	Manage SMS folders
 Settings	Change SMS settings
 New SMS/MMS	Create new SMS/MMS messages
 Reply	Reply to SMS
 Forward	Forward SMS
 Move to...	Move SMS to a folder
 Delete	Delete SMS
 Send/Recv	Send and receive SMS/MMS (if supported)
 Addresses	Manage Phone book contacts on SIM

A. Folder

By using this menu, you may change the folder structure of the SMS Center:



Button	Description
New Folder	Creates a new folder, name has to be unique
Rename	Renames an existing folder
Remove	Removes an existing folder (including the messages)

NOTE: Predefined folder can't be deleted or modified.

B. Settings

The settings window lets you change the deletion mode. You may choose whether to delete an SMS from the SMS Center, from the SIM or decide whether this should be asked at all. You may also activate an alarm signal when a new SMS arrives.

C. New SMS

The “New Message” window is used to enter the SMS text. You may also enter texts by copy & paste from other applications. The status bar at the lower right corner indicates the length of the SMS for your convenience: the first number tells you how many parts the SMS consists of (one part has max. 160 characters/unicode70), the second number counts down from 160/70 characters. The number in parenthesis () counts the total number of characters.

The recipient for your SMS has to be entered in the “To” field. This can be either entered by typing digits or by clicking the “To” button to select a recipient from the address book.

Recipient addresses may be taken from the SIM address book or from your email client’s contact folder. Just select an address and click OK. To send the message click “Send/Receive”.

D. Reply

Highlight a message to which you want to reply, e.g. in the inbox folder, then click the “Reply” button. The “New Message” window opens and the recipient address is already filled in the “To” field. Continue as before when sending a new message.

E. Forward

Highlight a SMS, which you want to forward. Click the “Forward” button. The “New Message” window opens, however the message text is already copied. Continue as before when sending a new message.

F. Move SMS...

Highlight the SMS to be moved and click the “Move SMS” button. A small window opens that lets you select the destination folder. Select the folder to which the message should be moved, then click “Move”.

G. Delete

Highlight the SMS which you want to delete. Click “Delete” to remove the message.

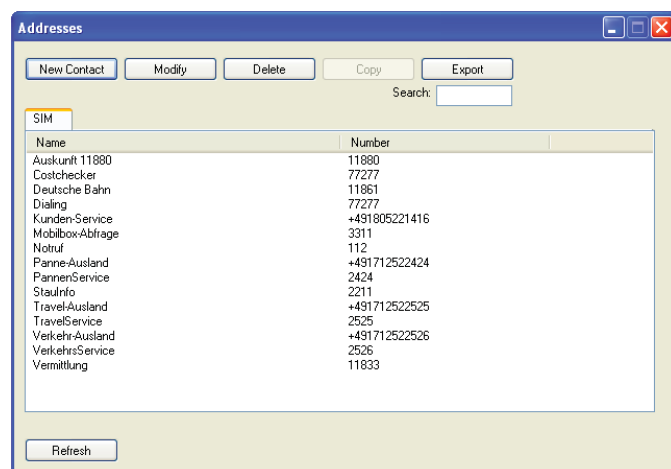
H. Send/Receive

Messages will be sent and/or received by clicking on this button.

I. Addresses

This button opens the address book. You may add new contacts to your personal address book or you may change existing addresses, delete addresses or exchange them with your SIM card and your e-mail client application, or export the data set.

Button	Description
New Contact	New Contact
Modify	Modify a contact
Delete	Delete contacts, mark one or more and press on the button
Copy	Synchronisation with MS Outlook
Export	To export addresses you may select between two export formats: <ul style="list-style-type: none">• CSV (comma separated text format, usually read by spread sheet applications)• VCard (business card format, used by MS Outlook and other applications)



Web Browser

This button allows the user to open the Web Browser and surf the Internet once the connection is established. The used browser will be the system default browser which is set in the System Internet options.

E-Mail

This button will open the E-Mail application once the connection is established. The used application will be the system default E-Mail client which is set in the System options.

GPS

Pressing the GPS button will lead you to the GPS Window. Press button ‘get GPS’ then GPS will be started, indicated by the rotating GPS button, to search for Latitude and Longitude Data.



If Latitude and Longitude Data are displayed, then the user can press the button 'Track Me' to open Google Maps showing him his Position on a map.

Latitude: Gives the location of a place on Earth (or other planetary body) north or south of the equator.

Longitude: is the geographic co-ordinates most commonly used in cartography and global navigation for east-west measurement.

6. Radio Button

The Radio button allows you to switch on and off the radio of your mobile broadband device to save power or to switch to airplane mode.



If the radio is switched off the button becomes red. If it is on, it is green. In case the radio is disabled by a hardware switch or if the device is not available, the button will be disabled.

7. Update

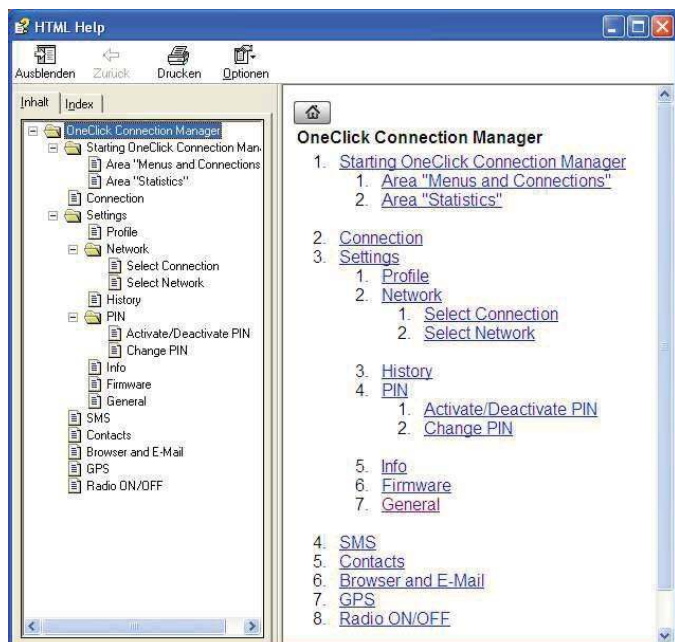
One Click Internet provides a build-in online update functionality that allows for an automatic update of OneClick Internet application, device drivers, and APN database.

The update is triggered by pressing the update button. The application will check on the WebToGo server, if updates are available, and offer them for download if suitable.

In order to start the update, select a file from the list of available updates and press OK.

8. Help

OneClick Internet provides a build-in online help that can be opened by pressing the help button on the main windows.



Web Browser

This button allows the user to open the Web Browser and surf the Internet once the connection is established. The used browser will be the system default browser which is set in the System Internet options.

E-Mail

This button will open the E-Mail application once the connection is established. The used application will be the system default E-Mail client which is set in the System options.

GPS

Pressing the GPS button will lead you to the GPS Window. Press button 'get GPS' then GPS will be started, indicated by the rotating GPS button, to search for Latitude and Longitude Data.



If Latitude and Longitude Data are displayed, then the user can press the button 'Track Me' to open Google Maps showing him his Position on a map.

Latitude: Gives the location of a place on Earth (or other planetary body) north or south of the equator.

Longitude: is the geographic co-ordinates most commonly used in cartography and global navigation for east-west measurement.

6. Radio Button

The Radio button allows you to switch on and off the radio of your mobile broadband device to save power or to switch to airplane mode.



If the radio is switched off the button becomes red. If it is on, it is green. In case the radio is disabled by a hardware switch or if the device is not available, the button will be disabled.

7. Update

One Click Internet provides a build-in online update functionality that allows for an automatic update of OneClick Internet application, device drivers, and APN database.

The update is triggered by pressing the update button. The application will check on the WebToGo server, if updates are available, and offer them for download if suitable.

In order to start the update, select a file from the list of available updates and press OK.

8. Help

OneClick Internet provides a build-in online help that can be opened by pressing the help button on the main windows.

