TL260GS/TL265GS

Ethernet/Internet and GSM/GPRS Dual-Path Alarm Communicator

GS2060/GS2065

GSM/GPRSGSM/GPRS Wireless Alarm Communicator

DSC®

Software Version 1.0

Installation Manual

Table of Contents

IMPORTANT

The equipment is fixed, wall-mounted and shall be installed in the position specified in these instructions. The equipment enclosure must be fully assembled and closed, with all the necessary screws/tabs and secured to a wall before operation. Internal wiring must be routed in a manner that prevents:

- **Excessive strain on wire and on terminal connections;**
- **Loosening of terminal; connections;**
- **Damage of conductor insulation**

WARNING: Never install this equipment during a lightning storm!

Instruct the end-user to:

- **Not attempt to service this product. Opening or removing covers may expose the user to dangerous voltages or other risks. Any servicing shall be referred to trained service personnel only.**
- **Use authorized accessories only with this equipment.**

Do not dispose of the battery in fire or water. Disposing of the battery in a fire will cause rupture and explosion;

Do not dispose of the waste battery as unsorted municipal waste. Consult your local regulations and / or laws regarding recycling with regard to this battery; Doing so will help protect the environment. Some of the materials that are found within the battery could become toxic if not disposed of properly and may affect the environment.

WARNING Please Read Carefully

Note to Installers

This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the users of this system.

System Failures

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some but not all of these reasons may be:

Inadequate Installation

A security system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a security professional to ensure that all access points and areas are covered. Locks and latches on windows and doors must be secure and operate as intended. Windows, doors, walls, ceilings and other building materials must be of sufficient strength and construction to provide the level of protection expected. A reevaluation must be done during and after any construction activity. An evaluation by the fire and/or police department is highly recommended if this service is available.

Criminal Knowledge

This system contains security features which were known to be effective at the time of manufacture. It is possible for persons with criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a security system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

Access by Intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.

Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment such as a security system. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

Failure of Replaceable Batteries

This system's wireless transmitters have been designed to provide several years of battery life under normal conditions. The expected battery life is a function of the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

Compromise of Radio Frequency (Wireless) Devices

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent radio signal interference.

System Users

A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm.

Smoke Detectors

Smoke detectors that are a part of this system may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fires equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

Warning Devices

Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

Telephone Lines

If telephone lines are used to transmit alarms, they may be out of service or busy for certain periods of time. Also an intruder may cut the telephone line or defeat its operation by more sophisticated means which may be difficult to detect.

Insufficient Time

There may be circumstances when the system will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.

Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

Inadequate Testing

Most problems that would prevent an alarm system from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an earthquake, an accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

Security and Insurance

Regardless of its capabilities, an alarm system is not a substitute for property or life insurance. An alarm system also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergencysituation.

Introduction

The GS2060/GS2065 Communicators are GSM/GPRS wireless alarm communicators that send alarm communication to Sur-Gard System I, II and III monitoring station receivers through the GSM/GPRS digital cellular network.

The TL206GS/TL265GS Communicators are dual-path alarm communicators that send alarm communication to Sur-Gard System I, II and III monitoring station receivers through the Ethernet/Internet or the GSM/GPRS digital cellular network.

The performance of the TL260GS/TL265GS/GS2060/GS2065 Communicator depends greatly on GSM network coverage. It should not, therefore, be mounted without first performing placement tests to determine the best location for reception (minimum of one green LED On). Optional antenna kits are available.

For UL Residential Fire and Burglary installations, the TL260GS/TL265GS/GS2060/GS2065 Communicator is listed as a primary (sole) communication means or as a backup when used in conjunction with a POTS line (dialer).

For UL Commercial Burglary installations, the TL260GS/TL265GS/GS2060/GS2065 Communicator is listed for supplementary (backup) use in conjunction with a POTS line (dialer).

Models

The following models are compatible with PC1616/PC1832/PC1864 control panels:

- **TL260GS (Ethernet + GSM/GPRS dual-path)**
- **GS2060 (GSM/GPRS only)**

The following models are compatible with PC9155 control panel:

- **TL265GS (Ethernet + GSM/GPRS dual-path)**
- **GS2065 (GSM/GPRS only)**

Features

- **Fully redundant Internet and GSM/GPRS dual-path alarm communication (TL265GS/TL260GS only)**
- **Back up or primary GSM/GPRS alarm communication**
- **Integrated call routing**
- **Panel remote uploading/downloading support via GSM/GPRS and Internet**
- **Supervision heartbeats via GSM/GPRS and Internet**
- **128-bit AES encryption via GSM/GPRS and Internet**
- **Full event reporting**
- **SIA format**
- **PC-Link connection**
- **Signal strength and Trouble display**
- **Activating and initializing through Connect 24**
- **Quad-Band: 850 MHz, 1900 MHz, 900 MHz and 1800 MHz**

Technical Specifications

The input voltage to the TL260GS/TL265GS/GS2060/GS2065 Communicator can be drawn from the UL/ULC Listed Control Panel or provided by an external UL Listed power supply rated for the application (external power-limited source).

NOTE: The power supply must be Class II, Power Limited.

Ratings

Table 1: Communicator Ratings

Model	GS2060 GSM/GPRS only	TL260GS Ethernet & GPRS	GS2065 GSM/GPRS only	TL265GS Ethernet & GPRS
Power Supply Ratings				
• Input Voltage	10 ~ 13.8V DC (From the Panel Bell output)		10V ~ 13.8V DC (From PC-Link Header)	
Current Consumption				
• Standby Current	65mA @ 12V	100mA @ 12V	65mA @ 12V	100mA @ 12V
• Alarm (Transmitting) Current	400mA during transmission			
• Operating Frequency	850/1900MHz ~ 900/1800MHz			
• Antenna Gain	2db			
Environmental Specifications				
• Operating Temperature	-10°C ~ 55°C (14°F ~ 131°F)			
• Humidity	5% ~ 93% RH non-condensing			
Mechanical Specifications				
• Board Dimensions (mm)	100 × 150 × 15	100 × 150 × 18	100 × 150 × 15	100 × 150 × 18
• Weight	310g	320g	68g	78g

NOTE: UL/ULC does not test below 0°C.

Compatibility

Table 2: Compatible Receivers, Control Panels, and Cabinets

Communicator	Receiver/Panel	Description
GS2060/TL260GS GS2065/TL265GS	Receiver	• Sur-Gard System I Receiver, version 1.10+ • Sur-Gard System II Receiver, version 2.00+ • Sur-Gard SG-DRL3-IP, version 2.20+ (for Sur-Gard System III Receiver)
GS2060/TL260GS	Control Panel and Cabinets	• Power Series PC1864, version 4.1+ • Power Series PC1832, version 4.1+ • Power Series PC1616, version 4.1+ • Cabinets: PC5003C/PC4050C
GS2065/TL265GS	Control Panel	• PC9155 version 1.0+

Installing the GSM/ETHERNET Communicator

This GSM/Ethernet Communicator is fixed and shall be installed by Service Persons only (Service Person is defined as a person having the appropriate technical training and experience necessary to be aware of hazards to which that person may be exposed in performing a task and of measures to minimize the risks to that person or other persons). It shall be installed and used within an environment that provides the pollution degree max 2, over voltages category II, in non-hazardous, indoor locations only. This manual shall be used with the Installation Manual of the alarm control panel which is connected to the GSM/Ethernet Communicator. All instructions specified within that manual must be observed.

All the local rules imposed by local electrical codes shall be observed and respected during installation.

Connect 24 Activation and Initialization

Installation of the Communicator requires activation with Connect 24 to operate. Dealer application forms and additional information on the Connect 24 Voice Response Unit (VRU) and web user-interface can be found at www.connect24.com or at the following telephone numbers:

USA 1-888-251-7458 CANADA 1-888-955-5583

IMPORTANT: Prior to installing a GS2060, TL260GS, GS2065 and TL265GS, contact your monitoring station to determine if it is a master re-seller or visit www.connect24.com and become an authorized dealer. In both instances, you will acquire a Profile Number, Installer ID Number and an Installer Password.

NOTE: You need to activate the SIM card and initialize the communicator 24 HOURS BEFORE INSTALLATION

1. **Retrieve the installer account and password from the master reseller, or from Connect 24 directly.**
2. **Go to the Connect 24 website (www.connect24.com).**

3. **Log in to the website using the installer account and password.**
4. **Activate the SIM card and initialize programming:**
   - **Go to the Initialize an account section.**
   - **Select Profile (This will be provided by the master reseller or by Connect 24).**
   - **Select Product Module.**
   - **Enter the SIM card number.**
   - **Enter related information as required.**
   - **Confirm all information before submitting.**
5. **Activate and initialize the programming of another SIM card (i.e. subscriber), or log out from the Connect 24 website.**

When you are at the physical installation site to install the Communicator and the control panel, the Communicator will automatically download its programming from Connect 24 once it is connected and turned on.

Following initial installation, you can log in to the Connect 24 website at any time to re-configure the Communicator remotely. For more information, see the Connect 24 website (www.connect24.com).

Establishing a communication channel between the Communicator and the PC9155 Panel

Establishing a communication channel between the Communicator and the panel is critical to ensuring the desired operation of the two units. These steps must be undertaken during the on-site installation.

1. **Proceed to Connect 24 Activation Information above.**
2. **Wire the telephone line, if available.**
3. **Wire the PC9155 panel (but *not* the Communicator).**
4. **Turn on the PC9155 panel. Program the panel's telephone number, account code, format, GS/IP module enable, and the communication path priority (i.e. PSTN → Ethernet → GRPS).**
5. **Turn off the panel.**
6. **Wire the Communicator through the PC-Link.**

Prior to on-site installation, visit the Connect 24 website (www.connect24.com) or telephone the Connect 24 Voice Response Unit (VRU) at 1-866-910-3865 to activate the SIM card and initialize programming of the Communicator.

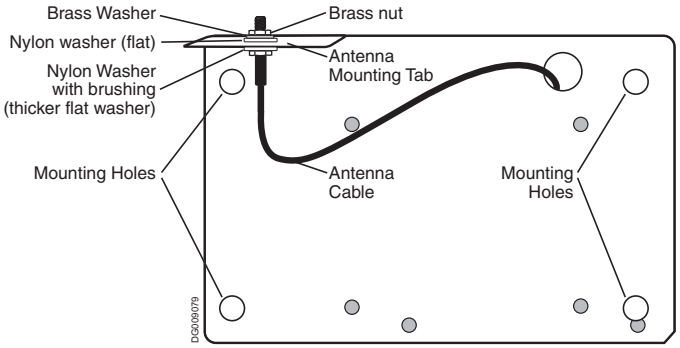
NOTES: Keep a record of the SIM card number for future reference.
Due to the nature of the SIM card activation process with GSM network carriers, it can take up to 24 hours for SIM card activation to be complete.

Installation with PC1616/1832/1864 Control Panel (models TL260GS and GS2060)

NOTE: For installation with the PC9155 Control Panel, see Installation with PC9155 Control Panel (models TL265GS and GS2065) on page 6.

1. **Assemble the Communicator**
   - **Remove the four white plastic standoffs from their bag in the Communicator kit.**
   - **Insert the standoffs in through the back (the antenna mounting tab will be facing away from you) of the supplied bracket, using the four holes provided for that purpose located at each of the four corners of the bracket.**
   - **Place the bracket on a solid surface. Grasping the edges of the PCB, keeping the board face up, orient the four holes on the PCB with the four standoffs protruding from the bracket. Push the PCB firmly and evenly onto the standoffs until the PCB is secured to the bracket.**
   - **Remove the antenna cable, white whip antenna, brass washer, nylon washer with bushing (thick flat washer), nylon washer (flat), and brass nut from their bag.**
   - **Connect the supplied 12.7cm (5") antenna cable to the radio by inserting the connector through to the Communicator board from the back of the bracket, and then pushing the connector firmly into the socket on the radio.**
   - **Place the nylon washer with bushing (thick flat washer) onto the threaded section of the cable. Insert the threaded section up through antenna mounting tab. Place the second nylon washer (flat), followed by the brass washer and the brass nut, onto the threaded section of the cable. Tighten the assembly by hand.**

NOTE: Ensure the SIM card is inserted on the communicator



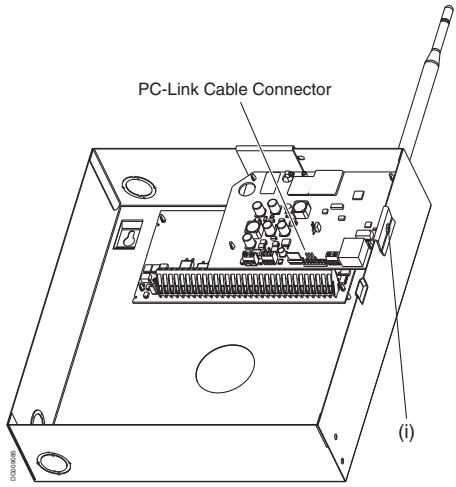
2. Install the Communicator module into the Cabinet

NOTE: Before installing the TL260GS/GS2060 or inserting/removing the SIM card, ensure that the system is turned off.

- **Remove the cabinet's front cover.**
- **Remove the circular knockout located in the top-right section of the cabinet. This knock-out will be used for connection of the supplied antenna.**
- **Attach the 4-pin PC-Link cable connector to the panel board.**

NOTE: Note that the red wire is on the right and the black wire is on the left, whereas on the Communicator this is reversed.

- **Insert the Communicator into the panel cabinet.**
- **Locate the screw hole in the right hand wall of the panel. Line up the bracket and the side wall and, using the screw provided, affix the two together (i). Ensure that the threaded antenna connection point appears through the knockout hole of the cabinet.**



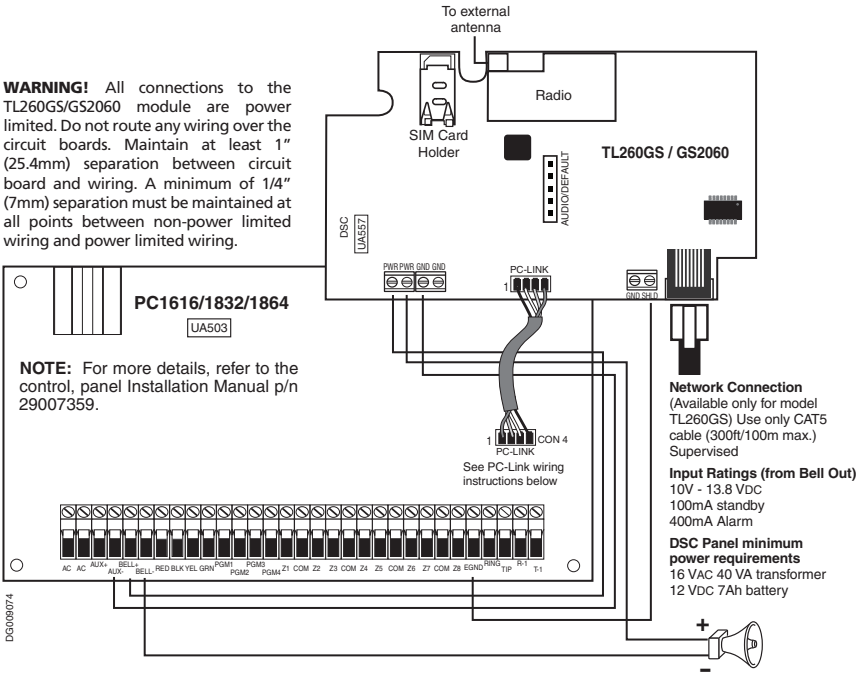
- **There are four terminals on the Communicator available for power connection, labeled PWR PWR GND GND.**
- **Attach either one of the two PWR terminals to the panel's BELL+ terminal.**
- **Attach the other PWR terminal to the Bell; also, attach the panel's BELL- terminal to the Bell.**
- **Attach the Communicator's GND terminal to the panel's AUX- terminal.**
- **Locate the 2-terminal block labeled GND SHLD. The SHLD terminal must be wired to the cabinet's protective earth ground (EGND).**
- **In the cabinet, locate the plug for the Ethernet cable and affix.**
- **Reassemble the PC1864 cabinet.**
- **Attach the supplied antenna onto the antenna connector at the top right-hand side of the cabinet. Care must be taken not to overtighten the antenna, as damage to the antenna may occur as a result.**
- **Finally, insert the SIM card.**

NOTE: The installation procedure for the GS2060 is identical to the above, with the exception that it does not have the Ethernet option.

3. Turn on the panel and check signal strength.

- **Turn on the unit.**
- **The green LEDs on the Communicator board will indicate the signal strength. The right-hand green LED must be On and solid - not flashing - for the location to be acceptable. Please refer to STATUS LEDs on page 8 for more information.**

TL260GS/GS2060 Communicator Wiring Diagram



WARNING! All connections to the TL260GS/GS2060 module are power limited. Do not route any wiring over the circuit boards. Maintain at least 1" (25.4mm) separation between circuit board and wiring. A minimum of 1/4" (7mm) separation must be maintained at all points between non-power limited wiring and power limited wiring.

NOTE: For more details, refer to the control, panel Installation Manual p/n 29007359.

Network Connection
(Available only for model TL260GS) Use only CAT5 cable (300ft/100m max.) Supervised

Input Ratings (from Bell Out)
10V - 13.8 VDC
100mA standby
400mA Alarm

DSC Panel minimum power requirements
16 VAC 40 VA transformer
12 VDC 7Ah battery

NOTE: For ULC Commercial Fire Monitoring applications, do NOT connect any devices on the Bell+ terminal other than the TL260GS/GS2060.

Wiring the TL260GS/GS2060 Module to a PC1616/1832/1864

- **Remove the circular knock out in the top right-hand corner of the cabinet and mount the TL260GS/GS2060 module in place (secure using screws supplied).**
- **Attach the TL260GS/GS2060 antenna to the unit.**
- **With both the AC and battery disconnected from the DSC control panel, wire the supplied PC-Link cable.**
- **Wire the Bell+ of the control panel to the TL260GS/GS2060 PWR terminal.**
- **Wire the AUX- on the control panel to the TL260GS/GS2060 GND.**
- **Apply AC and DC to the main control panel, the TL260GS/GS2060 and the PC1616/1832/1864 should power up.**
- **Perform the necessary programming.**

NOTE: If a Bell/Siren is not being used, wire the Bell/Siren terminals on the panel with a 1K ohm resistor, then only wire the BELL+ to the PWR of the TL260GS/GS2060.

Connecting the PC-Link Cable

- **Insert the connector on the TL260GS/GS2060 with the black wire on Pin 1 of the PC-Link header.**
- **Insert the other end of the cable on the PC1616/1832/1864 with the red wire on Pin 1 of the PC-Link header.**

Before leaving the premises the Ethernet communication lines must first be connected to an approved (acceptable to local authorities)type NID device, (UL installations, UL 60950 listed NID, for ULC installations CAN/CSA C22.2. No. 60950-1 Certified NID).

Optional Antenna Kits

The PC1616/1832/1864 cabinet contains an external GSM radio antenna. If the required GSM signal strength cannot be achieved using this antenna, the following selection of GSM extension antenna kits are available to the installer:

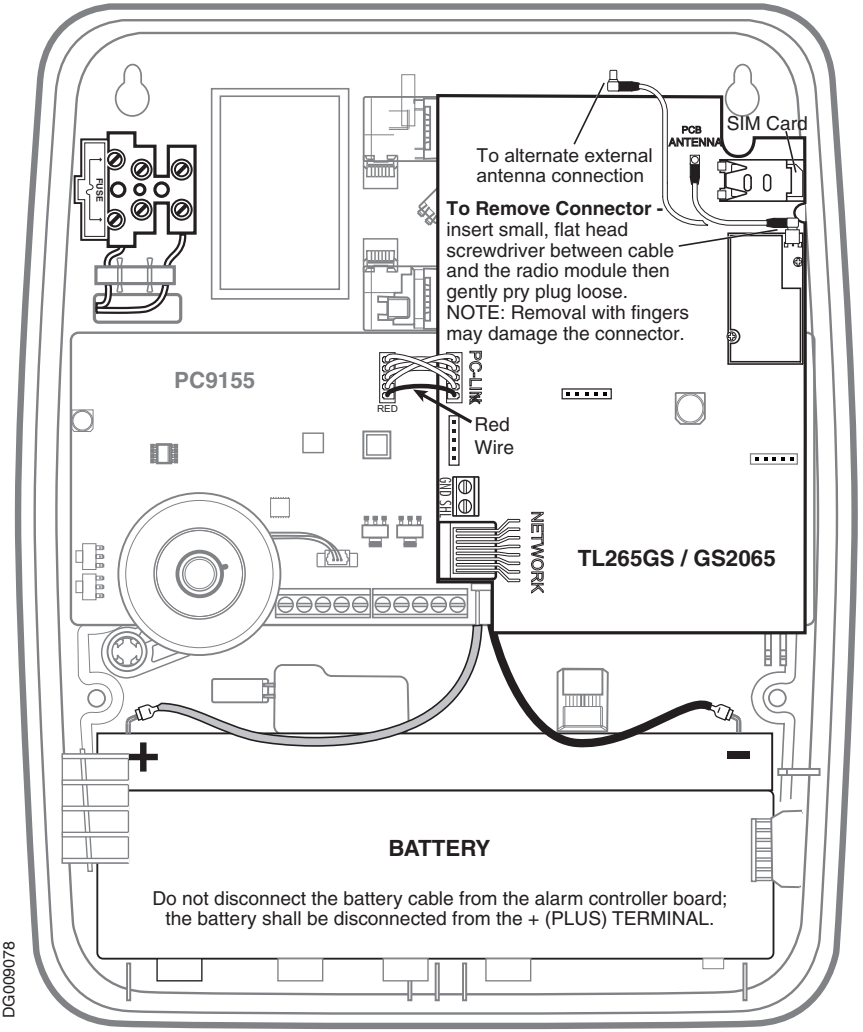
- **GS15-ANTQ - 4.57m (15') Internal Antenna Extension Kit (suitable for interior mounting only)**
- **GS25-ANTQ - 7.62m (25') External Antenna Extension Kit (suitable for exterior mounting only)**
- **GS50-ANTQ - 15.24m (50') External Antenna Extension Kit (suitable for exterior mounting only)**

Specific instructions for the installation of each extension antenna are included with each kit.

Installation with PC9155 Control Panel (models TL265GS and GS2065)

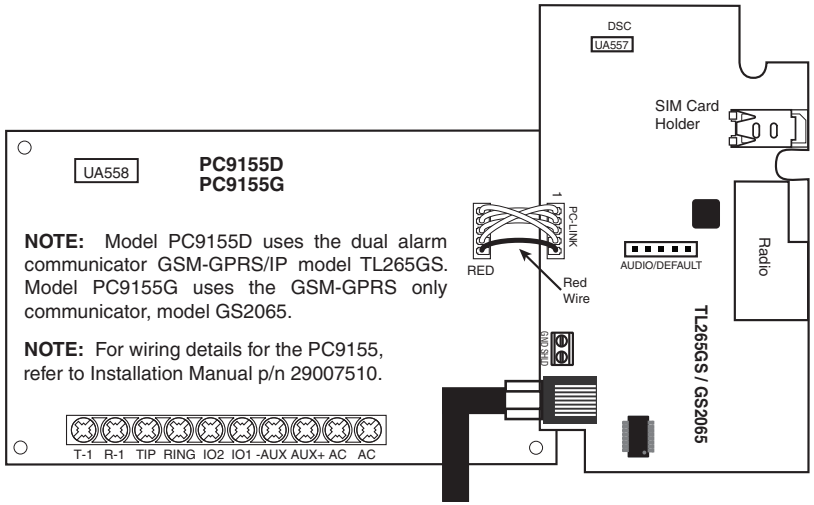
1. **Attach the Communicator to the inside of the PC9155 control panel cabinet if not already present.**
   NOTE: Install the TL265GS/GS2065 before turning on the system.
   NOTE: Before inserting or removing the SIM card, please ensure the unit is turned off.
   - **Separate the cabinet covers and place the Communicator in the space provided.**
   - **Attach the 5-pin PC-Link cable to the panel (see diagram on following page for orientation).**
   - **Locate the Ethernet jack on the Communicator and plug in the cable.**
   - **Locate the 2-terminal block (beside the Ethernet jack) labeled GND SHLD; it is optional to attach a short wire between these two terminals for noise reduction if a shielded network cable is used.**
   - **Insert the SIM card.**

   NOTE: Do not attach this wire if the cable shield is already grounded by the equipment at the other end.



2. **Turn on the PC9155 cabinet and check signal strength.**
   - **Turn on the unit.**
   - **The green LEDs will indicate the signal strength. The bottom green LED must be On and solid - not flashing - for the location to be acceptable. Please refer to STATUS LEDs on page 8 for more information.**

TL265GS/GS2065 Communicator Wiring Diagram



Optional Antenna Kits

The PC9155 enclosure contains an internal GSM radio antenna. If the required GSM signal strength cannot be achieved using the internal GSM antenna, the following selection of GSM extension antenna kits are available to the installer:

- **GS15-ANTQ - 4.57m (15') Internal Antenna Extension Kit (suitable for interior mounting only)**
- **GS25-ANTQ - 7.62m (25') External Antenna Extension Kit (suitable for exterior mounting only)**
- **GS50-ANTQ - 15.24m (50') External Antenna Extension Kit (suitable for exterior mounting only)**

Specific instructions for the installation of each extension antenna are included with each kit. Observe all the electrical safety instructions regarding the installation of the antennas; All the wiring of the equipment shall be fully compliant with the local rules and regulations.

PC1616/PC1832/PC1864 Programming

In order that your Communicator and your panel operate correctly together, specific panel options must be set. Take the following steps to ensure that your Communicator and your panel work together as intended.

These options must be set at the panel keypad.

1. **Program the hexadecimal digits (DCAA) in the telephone number that will be used for the GPRS/Ethernet Communicator (panel Options [301], [302], [303], 'Telephone Phone Number Programming').**
   Options [301], [302], [303]
   - **If a legitimate telephone number is entered in these options, you must use PSTN. If a legitimate telephone number is *not* used, you must use DCAA and route through the Communicator.**
   - **Options [301] is Primary communication path, and may be configured either as PSTN or DCAA. Option [302] is redundant, and Option [303] is the backup telephone number to Option [301].**

   NOTE: The leading digit 'D' in the telephone number for dial tone detection is pre-programmed.
2. **In Option [350], program the communication format as SIA FSK.**
   Option [350]: If Option [301] (above) is set to DCAA, Option [350] must be set to SIA.
3. **In Options [351] through Option [376], program the call direction sub-options for the phone number being used to communicate using the GPRS/Ethernet Communicator.**
4. **Option [382], sub-option [5], 'PC-Link Active' must be set to ON.**
5. **Option [167]: Set the value of this option to 60 seconds.**

PC9155 Programming

Specific panel options must be set for the correct operation of the Communicator.

1. **With the PC9155 panel, four telephone lines are available to backup one another. You can set up these four lines to perform in one of two ways: Backup dialling or Alternate dialling.**
   - **In the case of Backup dialling, each of the four telephone lines will make five dialling attempts in turn, before a FTC (Failure to Communicate) trouble is generated to the keypad.**
   - **In the case of Alternate dialling, each line makes one dialling attempt before moving on to the next line, cycling through the four lines for a total of five times each. At that point, an FTC trouble is made to the keypad.**

   You can choose from among five different paths, according to your particular system requirements:
   - **DCAA - Internal (Ethernet 1, Ethernet 2, GPRS 1, GPRS 2)**
   - **DCBB - Ethernet 1**
   - **DCCC - Ethernet 2 (backup)**
   - **DCDD - GPRS 1**
   - **DCEE - GPRS 2 (backup)**

   NOTE: Add a single 'F' as a suffix to the entry to populate the remainder of the unused field.

   Options [301], [302], [303], [305]
   - **If a legitimate telephone number is entered in these options, signal will be communicated using PSTN. If DCAA is entered, signals will be sent to Ethernet Receiver 1, DCCC = Ethernet Receiver 2, DCDD = GPRS Receiver 1, DCEE = GPRS Receiver 2.**
   - **Options [301], [302], [303] and [305] can be configured as Primary communication paths. Options [302], [303] and [305] may also be configured for backup or redundant communications by using Options [383] or [351] to [376]. Please refer to PC9155 Installation Manual for more information.**
2. **Option [350]: If Option [301] (above) is set to DCAA, Option [350] must be set to SIA.**
3. **Option [382]: sub-option [5], 'GS/IP Module Enabled', must be set to On. If this option is Off, the status LED will indicate the "Panel Supervision Trouble" and the unit could not be programmed via PC-Link cable.**
4. **Option [167]: Set the value of this option to 60 seconds.**

STATUS LEDs

The module has four onboard surface mount LED indicators. These include a Trouble Status LED on page 8, a Network Connection Status LED on page 9, and two Signal Strength LEDs on page 9.

Trouble Status LED

This Yellow LED will flash to indicate a trouble on the unit. The number of flashes indicates the type of trouble. See the table below for the types of conditions which will activate the Trouble Status LED.

Table 3: Trouble Status LED

# of Flashes	Trouble	# of Flashes	Trouble
1	Reserved	7	Receiver Not Available
2	The following conditions will cause this trouble to indicate:	8	Receiver Supervision Trouble
3	Reserved	9	FTC Trouble
4	SIM Lock Trouble	10	Connect 24 Configuration SMS Failure
5	GSM Trouble	11	Remote Programming
6	Ethernet Trouble	12	Remote Firmware Update Pending

The following conditions will cause this trouble to indicate:

Panel Supervision Trouble

This trouble will be indicated when communication between the Communicator module and the control panel fails. If for some reason the the module can not communicate with the panel - eg, loss of power to the panel - the module itself will send a 'Panel Absent Trouble Event' message to the central station receiver. When communication returns, a 'Panel Absent Restore Event' is sent by the module to the central station receiver. Its reporting codes are ET0001 for Trouble, ER0001 for Restore.

NOTE: The Panel Supervision Trouble/Restore is an internal event. It is the only internal event; all other events are external.

SIM Lock Trouble

This trouble will signify that the SIM lock feature has been enabled and the unit has not been programmed with the correct PIN for the SIM card. SIM Card Lockout Trouble equates to SIM Lock Trouble or Network Lock Trouble.

Network Carrier Lock Trouble

This trouble will be indicated when the device has been locked to operate on a specific network and the SIM card inserted in the device does not belong to the network the device is locked to.

GSM Trouble

This trouble is indicated for any one of the three following conditions: Radio or SIM Failure; GSM Network Trouble; Insufficient Signal Strength.

Ethernet Trouble

This trouble is indicated when the Ethernet link between the transmitter and the local hub or router is absent. In addition, this trouble will be indicated if the unit fails to receive an IP address from the DHCP server.

Receiver Not Available

This trouble is triggered if the unit is not able to successfully initialize with any of the programmed receivers.

Receiver Supervision Trouble

This trouble is indicated when receiver supervision is enabled and communication between the communicator module and the receiver fails.

FTC Trouble

This trouble is indicated when the unit fails to communicate module events to the central station.

Connect 24 Configuration SMS Failure

This trouble is indicated when the unit fails to receive programming from Connect 24.

Remote Programming

This indication is displayed during a remote firmware upgrade.

Network Connection Status LED

The normal state of the Red Network Connection Status LED is Off when there are no network connection issues present.

This LED will activate when there is an issue with either the Ethernet or the GPRS network connection. This LED will be triggered:

- **If the physical Ethernet cable is not connected**
- **If the DHCP configuration fails**
- **If the unit fails to get an IP address from the GPRS network**
- **When the GPRS connection has been reset**

Signal Strength LEDs

The two Green signal strength LEDs are used to display the radio's signal strength.

Green 1 **, Green 2**  **.**

Table 4: Radio Signal Strength

Signal Strength	Description	db Levels	Response
None	Green1 - Off; Green2 - Off; Yellow - On	-100db and lower	The unit must be relocated
Low	Green1 - Flashing; Green2 - Off	-99db to -92db	Relocate the unit, if possible.
Medium	Green1 - On; Green2 - Off	-91db to -77db	Unit placement is acceptable.
Full	Green1 - On; Green2 - On	-76db and higher	Unit placement is acceptable.

NOTE: If during installation the radio signal strength weakens, the unit must be relocated. Should relocation of the unit be insufficient in improving the radio signal strength, an antenna extension may be added.

Adding an Antenna Extension

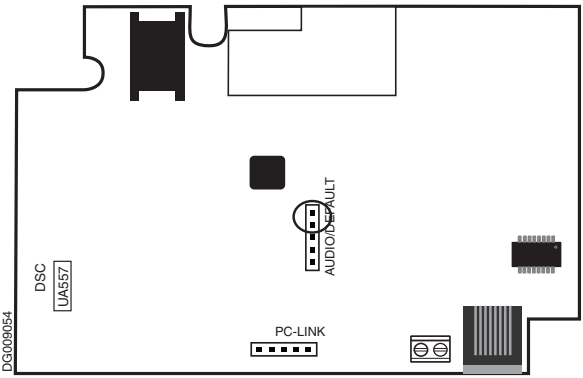
In the case of poor signal strength, an Antenna Extension Bracket kit may be required to rectify it. Take the following steps to install an antenna extension kit:

1. **Turn off the power to the Communicator by physically unplugging the unit from its power supply.**
2. **Attach one end of the extension cable to the Communicator and the other end to the antenna itself.**
3. **Reattach the power supply and turn on.**
4. **Move the antenna around until you have received a strong signal.**
5. **Mount the antenna bracket at that location.**

Hardware Default Jumper

You can reset the programming options for the Communicator to the factory settings. Take the following steps to reset your Communicator's programming options to their default settings.

1. **Locate the set of five pins in the middle of the Communicator board labeled AUDIO/DEFAULT. In the PC1616/1832/1864 panels these pins will be vertically aligned; In the PC9155 enclosure, these pins will be horizontally aligned.**



2. **Counting from the bottom, the first three pins are reserved for future use. You may discount these.**
3. **The final two pins require a jumper in order to reset the hardware values.**
4. **Turn off power to the Communicator.**
5. **Apply the jumper to the two pins.**
6. **Turn on power to the Communicator. Wait for ten seconds.**
7. **Remove the jumper from the pins.**

The programming options of your Communicator have now been reset to their default values.

Communicator Troubles on a PC9155 Panel

The following troubles will appear on the keypad LCD when encountered by a Communicator on the PC9155 panel.

Table 5: Communicator Troubles on a PC9155 Panel

Trouble Condition	Description	User Action
Alternate Communicator Trouble	GSM trouble, Ethernet trouble, Central station receiver trouble, supervision config SMS trouble for GS/IP module (if installed). Press < > to scroll through troubles.	Call for service. For Ethernet trouble check LAN connections.

Communicator Troubles on a PC1616/1832/1864 Panel

The General System trouble is the sole trouble that will appear on the keypad LCD when encountered by a Communicator on the PC1616/1832/1864 panel.

During the Software Update:

The unit can be updated through the DLS IV software.

- **When the firmware update begins, all LEDs are On.**
- **During the firmware update process, the LEDs will be cycled through individually.**
- **After a successful update the unit will restart.**
- **Should the update fail, the unit LEDs will turn On, then Off at one-second intervals.**
- **In this eventuality, restart the unit. In the event of consistent update failures, contact your dealer.**

Encryption

128 bit encryption can only be enabled from the monitoring station receiver. Each receiver can have encryption enabled or disabled. When encryption is enabled after the communicator has already communicated to that receiver, the packets will be start being encrypted only once the next event is sent to that receiver, or if the unit is re-started.

Power Save Mode and DLS

On the TL265GS model only, if there is an AC power loss on the PC9155 control panel, the system will enter a power save mode to extend battery duration. During that mode, the Ethernet functionality is turned off and will only turn on if an event needs to be transmitted. Therefore, incoming DLS connection will not be possible unless initiated through an SMS message. The Link activity LED on the network interface device will also be off during that time

Options

These options are programmed through Connect 24.

System Options

[001] Ethernet IP Address

Default (192.168.0.99)

NOTE: If Option [001] is set to '0.0.0.0', DHCP will set all values for the Ethernet IP Address, Subnet Mast, and Gateway.

Enter the IP address of the dual communicator. Take care to ensure that the IP address is unique to your communicator on the local network. The IP address must be entered as a dotted decimal number (e.g. 192.168.1.100). Each 3-digit segment of the IP address must be within a valid range of 000 to 255.

[002] Ethernet IP Subnet Mask

Default (255.255.255.000)

Enter the Ethernet IP Subnet Mask address of the dual communicator. The subnet mask must be entered as a dotted decimal number (e.g. 255.255.255.000). Each 3-digit segment of the address must be within a valid range of 000 to 255.

[003] Ethernet Gateway IP Address

Default (0.0.0.0)

Enter the Ethernet Gateway IP address of the dual communicator. The address must be entered as a dotted decimal number (e.g. 192.168.1.100). Each 3-digit segment of the address must be within a valid range of 000 to 255. The gateway is used in the event that the destination address is not on the local network. The data will need to be sent through a router device. This is the address of that router device.

[004] Heartbeat Interval

Default (0000)

When receiver supervision is enabled (Option [005], bit 1 and bit 2) the unit sends heartbeats to Ethernet Receiver 1 and GPRS Receiver 1 to indicate that it is still running. Use Option [004] to set the interval time at which heartbeats are sent. Heartbeat Interval window times are listed in the following table.

Table 6: Window Times

Jurisdiction	Receiver Window	Recommended Values
UL Commercial Burglary	200sec	155
UL Residential Fire	30 days	N/A
UL Residential Burglary	200 sec	155
ULC Commercial Burglary Active/Passive	180sec w/90sec heart-beats / 24hrs	45sec / 24hrs
ULC Commercial Fire Active/Passive	180sec / 24hrs	135 sec / 24hrs

[005] System Toggle Options

Default ( )

Table 7: System Toggle Options

Valid Data Range	Effect	Default
Bit 1	Ethernet Receiver 1 Supervised*	Disabled (Off)
Bit 2	GPRS Receiver 1 Supervised*	Disabled (Off)
Bit 3	Supervision Type: On - Commercial Supervision Off - Residential Supervision	Disabled (Off)
Bit 4**	Off - Ethernet channel is the primary path, GPRS channel is the secondary path On - GPRS channel is the primary path, Ethernet channel is the secondary path	Disabled (Off) - *Ethernet is primary, GPRS is secondary*
Bit 5	Redundant Communications - sends events at the same time over receivers 1 and 3, 2 and 4 (Ethernet/GPRS)	Disabled (Off)
Bit 6	Remote Firmware Upgrade - via Ethernet	Enabled (On)
Bit 7	Reserved	Disabled (Off)
Bit 8	Reserved	Disabled (Off)

****** Receivers 1 and 3 can be supervised; if enabled, heartbeats are sent. Receivers 2 and 4 cannot be supervised.***

****** Bit 4: When the communicator receives an SMS request to connect to DLS, it will use the primary path first to connect to DLS, and if that fails, will try the secondary path.***

Programming Options

[011] Installer Code

Default (CAFE)

This option is used to program the installer code of the Communicator module. Valid entries range from 0000 to FFFF hexadecimal.

[012] DLS Incoming Local Port

Default (3062)

The DLS Port is the port DLS IV will use when connecting to the Communicator. The router or gateway must be programmed with a TCP port forward for the communicator module. Valid entries range from 0000 to FFFF hexadecimal.

[013] DLS Outgoing Local Port

Default (3066)

The DLS local port is used when the Communicator is connecting to DLS IV after the SMS request has been sent to the communicator.. You can use this option to set the value of the local outgoing port. This should be used if the communicator is located behind a firewall and must be assigned a particular port number, as determined by your network administrator. In most cases, changing the default value or configuring your firewall with this port is not required. Valid entries range from 0000 to FFFF hexadecimal.

Ethernet Receiver 1 Options

(Required for TL260GS/TL265GS only.)

[101] Ethernet Receiver 1 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting heartbeat signals or panel absent/restore events to the central station receiver. Signals received from the control panel will use the control panel account number. Valid entries will range from 0000000000 to FFFFFFFFFF hexadecimal.

NOTE: If both, Ethernet receiver 1 and GPRS Receiver 1 are the same receiver (IP and port are identical), only Ethernet receiver 1 account will be used for both. Account 0000000000 and FFFFFFFFFF are not considered valid account numbers and can not be used.

[102] Ethernet Receiver 1 DNIS

Default (000000)

The DNIS is used in addition to the Account Code to to identify the Communicator module as the central station. Valid entries range from 000000 to 0FFFFF hexadecimal.

[103] Ethernet Receiver 1 IP Address

Default (127.0.0.1)

Enter the Ethernet receiver 1 IP address. This information will be provided by your central station. Note that when a valid address has been entered, the Ethernet will be considered to be enabled and will communicate events over the Ethernet channel. The address must be entered as four 3-digit entries (e.g. 192.168.1.101). Each 3-digit segment of the address must be within a valid range of 000 to 255.

Keeping the default loopback IP address (127.0.0.1) will allow the Ethernet path to be used for DLS only. Programming the Ethernet Receiver 1 IP address with 127.0.0.1 enables the Communicator to operate in Unattended Mode. Unattended Mode is used when a receiver is not available and the unit is required to perform DLS sessions. A typical application is an installation where the customer programs the control panel daily due to access control and still wants to receive alarms without buying extra hardware (receiver) or software. Programming the Ethernet receiver 2 IP address as 0.0.0.0 will disable Ethernet.

[104] Ethernet Receiver 1 Local Port

Default (0BF4 / 3060)

You can use this option to set the value of the local outgoing port. You can set the value of this port in case your installation is located behind a firewall and must be assigned a particular port number as determined by your network administrator. Valid entries range from 0000 to FFFF hexadecimal.

[105] Ethernet Receiver 1 Remote Port

Default (0BF5 / 3061)

Option [105] determines the port of Ethernet receiver 1. Valid entries range from 0000 to FFFF hexadecimal.

Ethernet Receiver 2 Options

(Required for TL260GS/TL265GS only.)

[111] Ethernet Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting heartbeat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid entries will range from 0000000000 to FFFFFFFFFF hexadecimal.

NOTE: If both, Ethernet receiver 2 and GPRS Receiver 2 are the same receiver (IP and port are identical), only Ethernet receiver 2 account will be used for both.

[112] Ethernet Receiver 2 DNIS

Default (000000)

The DNIS is used in addition to the Account Code to to identify the Communicator module as the central station. Valid entries range from 000000 to 0FFFFF hexadecimal.

[113] Ethernet Receiver 2 IP Address

Default (0.0.0.0)

Enter the Ethernet receiver 2 IP address. This information will be provided by your central station. Note that when a valid address has been entered, the Ethernet will be considered to be enabled and will communicate events over the Ethernet channel. The address must be entered as four 3-digit entries (e.g. 192.168.1.101). Each 3-digit segment of the address must be within a valid range of 000 to 255.

[114] Ethernet Receiver 2 Local Port

Default (0BF9 / 3065)

You can use this option to set the value of the local outgoing port. You can set the value of this port in case your installation is located behind a firewall and must be assigned a particular port number as determined by your network administrator. Valid entries range from 0000 to FFFF hexadecimal. Do not program Ethernet Receiver 1 Local Port and Ethernet Receiver 2 Local Port with the same value.

[115] Ethernet Receiver 2 Remote Port

Default (0BF5 / 3061)

Option [115] determines the port of Ethernet receiver 2. You can set the value of this port in case your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid entries range from 0000 to FFFF hexadecimal.

GPRS Receiver 1 Options

[201] GPRS Receiver 1 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting heartbeat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid entries will range from 0000000000 to FFFFFFFFFF hexadecimal.

[202] GPRS Receiver 1 DNIS

Default (000000)

The DNIS is used in addition to the Account Code to to identify the Communicator module as the central station. Valid entries range from 000000 to 0FFFFF hexadecimal.

[203] GPRS Receiver 1 IP Address

Default (0.0.0.0)

Enter the GPRS receiver 1 IP address. This information will be provided by your central station. Note that when a valid address has been entered, the GPRS will be considered to be enabled and will communicate events over the GPRS channel. The address must be entered as four 3-digit entria

es (e.g. 192.168.1.101). Each 3-digit segment of the address must be within a valid range of 000 to 255.

[204] GPRS Receiver 1 Remote Port

Default (0000)

Option [204] determines the port of GPRS receiver 1. You can set the value of this port in case your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid entries range from 0000 to FFFF hexadecimal.

[205] GPRS Receiver 1 APN

Default ( )

The APN (Access Point Name) identifies the GPRS network the communicator will connect to. This information is available from your network carrier.

GPRS Receiver 2 Options

[211] GPRS Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting signals to the central station receiver. Signals received on the control panel will use the control panel account number. Valid entries will range from 0000000000 to FFFFFFFFFF hexadecimal.

[212] GPRS Receiver 2 DNIS

Default (000000)

The DNIS is used in addition to the Account Code to to identify the Communicator module as the central station. Valid entries range from 000000 to 0FFFFF hexadecimal.

[213] GPRS Receiver 2 IP Address

Default (0.0.0.0)

Enter the GPRS receiver 2 IP address. This information will be provided by your central station. Note that when a valid address has been entered, the GPRS will be considered to be enabled and will communicate events over the GPRS channel. The address must be entered as four 3-digit entries (e.g. 192.168.1.101). Each 3-digit segment of the address must be within a valid range of 000 to 255.

[214] GPRS Receiver 2 Remote Port

Default (0000)

Option [214] determines the port of GPRS receiver 2. You can set the value of this port in case your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid entries range from 0000 to FFFF hexadecimal.

[215] GPRS Receiver 2 APN

Default ( )

The APN (Access Point Name) identifies the GPRS network the communicator will connect to. This information is available from your network carrier.

GPRS Options

[221] GPRS Public APN

Default ( )

When your communicator is operating on a private APN, you can use this option to switch to a public APN for DLS sessions. This information is available from your network carrier.

See [205] GPRS Receiver 1 APN above for more information on APNs.

[222] GPRS Login User Name

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Enter your login user name here.

[223] GPRS Login Password

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Enter your login password here.

System Information

Option

[991] Firmware Version

You can use this option to confirm the firmware version of the device.

[992] Ethernet IP Address

You can use this option to confirm the IP address of the Ethernet connection.

[993] Ethernet Gateway IP Address

You can use this option to confirm the IP address of the Ethernet Gateway.

[994] GPRS IP Address

You can use this option to confirm the IP address of the GPRS connection.

[995] SIM Number

You can use this option to confirm the SIM number of the device.

[996] GSM Phone Number

You can use this option to confirm the GSM telephone number of the device.

[997] IMEI Number

You can use this option to confirm the IMEI of the radio.

[998] MAC Number

You can use this option to confirm the MAC address of the device.

Programming Worksheets

System Options

[001] Ethernet IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[002] Ethernet IP Subnet Mask

|____|____|____|____|____|____|____|____|____|____|____|____|

[003] Ethernet Gateway IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[004] Heartbeat Interval

|____|____|____|____|

[005] System Toggle Options

|____| **Bit 1 - Ethernet Receiver 1 Supervised**
|____| **Bit 2 - GPRS Receiver 1 Supervised**
|____| **Bit 3 - Supervision Type**
|____| **Bit 4 - Primary Comms Channel**
|____| **Bit 5 - Redundant Communications**
|____| **Bit 6 - Remote Firmware Upgrade**
|____| **Bit 7 - Reserved**
|____| **Bit 8 - Reserved**

Programming Options

[011] Installer Code

|____|____|____|____|

[012] DLS Incoming Local Port

|____|____|____|____|

[013] DLS Outgoing Local Port

|____|____|____|____|

Ethernet Receiver 1 Options

[101] Ethernet Receiver 1 Account Code

|____|____|____|____|____|____|____|____|____|____|

[102] Ethernet Receiver 1 DNIS

|____|____|____|____|____|____|

[103] Ethernet Receiver 1 IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[104] Ethernet Receiver 1 Local Port

|____|____|____|____|

[105] Ethernet Receiver 1 Remote Port

|____|____|____|____|

Ethernet Receiver 2 Options

[111] Ethernet Receiver 2 Account Code

|____|____|____|____|____|____|____|____|____|____|

[112] Ethernet Receiver 2 DNIS

|____|____|____|____|____|____|

[113] Ethernet Receiver 2 IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[114] Ethernet Receiver 2 Local Port

|____|____|____|____|

[115] Ethernet Receiver 2 Remote Port

|____|____|____|____|

GPRS Receiver 1 Options

[201] GPRS Receiver 1 Account Code

|____|____|____|____|____|____|____|____|____|____|

[202] GPRS Receiver 1 DNIS

|____|____|____|____|____|____|

[203] GPRS Receiver 1 IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[204] GPRS Receiver 1 Remote Port

|____|____|____|____|

[205] GPRS Receiver 1 APN _____

GPRS Receiver 2 Options

[211] GPRS Receiver 2 Account Code

|____|____|____|____|____|____|____|____|____|____|

[212] GPRS Receiver 2 DNIS

|____|____|____|____|____|____|

[213] GPRS Receiver 2 IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[214] GPRS Receiver 2 Remote Port

|____|____|____|____|

[215] GPRS Receiver 2 APN _____

GPRS Options

[221] GPRS Public APN _____

[222] GPRS Login User Name _____

[223] GPRS Login Password _____

System Information

[991] Firmware Version

|____|____|____|____|____|____|____|____|

[992] Ethernet IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[993] Ethernet Gateway IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[994] GPRS IP Address

|____|____|____|____|____|____|____|____|____|____|____|____|

[995] SIM Number _____

[996] GSM Phone Number _____

[997] IMEI Number _____

[998] MAC Number _____

Appendix A: Troubleshooting

Indication	Trouble/Possible Causes	Possible Solution
No Indication – All indicators off	No Power	• Check your power connections to the control panel and the communicator module.
	Power Save Mode (TL265GS/ GS2065 only)	• The control panel may be in power save mode. Check the AC source to the control panel.
	Keypad Blanking Mode (TL265GS/GS2065 only)	• The control panel may be in keypad blanking. Press a key on a keypad to remove blanking momentarily.
Trouble LED – ON Solid	No Signal Strength	• Ensure the antenna is securely connected to the radio. Check the cable connection to the radio. • If a WIP antenna is used ensure the antenna is securely screwed on to the antenna cable connector.
Trouble LED – 2 Flashes	Panel Supervision Trouble	• Check section [382] option 5 on the control panel and ensure that it is set to "ON". • Ensure the PC-Link cable between the control panel and module is securely in place. • Ensure the PC-Link cable between the control panel and the module is not reversed.
Trouble LED - 4 Flashes	Lockout Trouble	• The SIM card requires a PIN number that the module does not know. Try a different SIM card. • The module has been locked to a specific carriers network and you are trying to use the device on an unsupported network. Use the device on the network it is intended to be used with.
Trouble LED – 5 Flashes	GSM Trouble	• Ensure the SIM card has been activated. • Ensure the SIM card is properly inserted into the SIM card holder. • Ensure there is adequate signal strength, by looking at the signal strength indicators. If not you will have to relocate the communicator module, or an external antenna extension kit may be used.
Trouble LED – 6 Flashes	Ethernet Trouble	• Ensure your Ethernet Cable is securely inserted into the Ethernet jack. • Check the link light on the HUB is in the "ON" state. If not try replacing the Ethernet cable. • If DHCP is used, ensure that the unit is successfully getting an IP address from the server. Enter section [851] [992] and verify a valid IP address is present. If not contact the Network administrator.
Trouble LED – 7 Flashes	Receiver Not Available	• Ensure the Ethernet path has internet connectivity. • If you are using a static IP address make sure the gateway is correct. • If the network has a firewall, ensure the network has the programmed outgoing ports open (Default UDP Port 3060 and Port 3065) • Ensure that all the receivers are programmed with the proper IP and port. • Ensure that all receivers are programmed with a valid account number.
Trouble LED – 8 Flashes	Receiver Supervision Trouble	• This trouble is indicated when supervision is enabled and the unit is not able to successfully communicate with the receiver. • If this trouble persists, contact your central station.
Trouble LED – 10 Flashes	Connect 24 Configuration Failure	• Ensure a profile has been programmed in Connect 24 for the module. • You can confirm your programming by calling the Connect 24 VRU, or by logging into the Connect 24 VRU web site.
All indicators flashing at the same time	Boot Loader Failed	• Disconnect then reconnect power to the communicator module.
Red and Yellow Indicator Flashing at the same time	Initialization Sequence	• The unit is still initializing please wait while the unit gets its programming from Connect 24 and establishes a connection to all programmed receivers. Note that this process may take several minutes.

IMPORTANT - READ CAREFULLY: DSC Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

- This End-User License Agreement ("EULA") is a legal agreement between You (the company, individual or entity who acquired the Software and any related Hardware) and Digital Security Controls, a division of Tyco Safety Products Canada Ltd. ("DSC"), the manufacturer of the integrated security systems and the developer of the software and any related products or components ("HARDWARE") which You acquired.
- If the DSC software product ("SOFTWARE PRODUCT" or "SOFTWARE") is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and "online" or electronic documentation.
- Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.
- By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, DSC is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE This EULA grants You the following rights:

(a) Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.

(b) Storage/Network Use - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device ("Device"). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.

(c) Backup Copy - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

(a) Limitations on Reverse Engineering, Decompilation and Disassembly - You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to the Software, without the written permission of an officer of DSC. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.

(b) Separation of Components - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.

(c) Single INTEGRATED PRODUCT - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.

(d) Rental - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.

(e) Software Product Transfer - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided You retain no copies, You transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades and this EULA), and provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT.

(f) Termination - Without prejudice to any other rights, DSC may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

(g) Trademarks - This EULA does not grant You any rights in connection with any trademarks or service marks of DSC or its suppliers.

3. COPYRIGHT - All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by DSC or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by DSC and its suppliers.

4. EXPORT RESTRICTIONS - You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to Canadian export restrictions.

5. CHOICE OF LAW - This Software License Agreement is governed by the laws of the Province of Ontario, Canada.

6. ARBITRATION - All disputes arising in connection with this Agreement shall be determined by final and binding arbitration in accordance with the Arbitration Act, and the parties agree to be bound by the arbitrator's decision. The place of arbitration shall be Toronto, Canada, and the language of the arbitration shall be English.

7. LIMITED WARRANTY

(a) NO WARRANTY - DSC PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. DSC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

(b) CHANGES IN OPERATING ENVIRONMENT - DSC shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-DSC-SOFTWARE or HARDWARE PRODUCTS.

(c) LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK - IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, DSC'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE CANADIAN DOLLARS (CAD$5.00). BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

(d) DISCLAIMER OF WARRANTIES - THIS WARRANTY CONTAINS THE ENTIRE WARRANTY AND SHALL BE IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED (INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) AND OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF DSC. DSC MAKES NO OTHER WARRANTIES. DSC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.

(e) EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY - UNDER NO CIRCUMSTANCES SHALL DSC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF THE SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY.

WARNING: DSC recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.

Limited Warranty

Digital Security Controls warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Digital Security Controls shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original purchaser must promptly notify Digital Security Controls in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period. There is absolutely no warranty on software and all software products are sold as a user license under the terms of the software license agreement included with the product. The Customer assumes all responsibility for the proper selection, installation, operation and maintenance of any products purchased from DSC. Custom products are only warranted to the extent that they do not function upon delivery. In such cases, DSC can replace or credit at its option.

International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Digital Security Controls shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- **damage incurred in shipping or handling;**
- **damage caused by disaster such as fire, flood, wind, earthquake or lightning;**
- **damage due to causes beyond the control of Digital Security Controls such as excessive voltage, mechanical shock or water damage;**
- **damage caused by unauthorized attachment, alterations, modifications or foreign objects;**
- **damage caused by peripherals (unless such peripherals were supplied by Digital Security Controls);**
- **defects caused by failure to provide a suitable installation environment for the products;**
- **damage caused by use of the products for purposes other than those for which it was designed;**
- **damage from improper maintenance;**
- **damage arising out of any other abuse, mishandling or improper application of the products.**

Items Not Covered by Warranty

In addition to the items which void the Warranty, the following items shall not be covered by Warranty: (i) freight cost to the repair centre; (ii) products which are not identified with DSC's product label and lot number or serial number; (iii) products disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection or testing to verify any warranty claim. Access cards or tags returned for replacement under warranty will be credited or replaced at DSC's option. Products not covered by this warranty, or otherwise out of warranty due to age, misuse, or damage shall be evaluated, and a repair estimate shall be provided. No repair work will be performed until a valid purchase order is received from the Customer and a Return Merchandise Authorisation number (RMA) is issued by DSC's Customer Service.

Digital Security Controls' liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty. Under no circumstances shall Digital Security Controls be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property. The laws of some jurisdictions limit or do not allow the disclaimer of consequential damages. If the laws of such a jurisdiction apply to any claim by or against DSC, the limitations and disclaimers contained here shall be to the greatest extent permitted by law. Some states do not allow the exclusion or limitation of incidental or consequential damages, so that the above may not apply to you.

Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) and of all other obligations or liabilities on the part of Digital Security Controls Digital Security Controls neither assumes responsibility for nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

WARNING: Digital Security Controls recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs

Digital Security Controls will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Digital Security Controls determines to be repairable will be repaired and returned. A set fee which Digital Security Controls has predetermined and which may be revised from time to time, will be charged for each unit repaired.

FCC Compliance Statement

CAUTION: Changes or modifications not expressly approved by the manufacturer could void your authority to use this equipment.

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 or more of the following measures:

- **Re-orient 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/television technician for help.**

The user may find the following booklet prepared by the FCC useful: "How to Identify and Resolve Radio/Television Interference Problems". This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, Stock # 004-000-00345-4.

Warning: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20cm or more must be maintained between the antenna of this device and persons during device operation.

Industry Canada Statement

The prefix 'IC:' in front of the radio certification number signifies only that Industry Canada technical specifications were met.

Certification Number IC: 160A-GS260L

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

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

29007516R001

DSC®

Toronto, Canada • **www.dsc.com**
Tech Support: 1-800-387-3630 (Canada & US) or 905-760-3036
Printed in Canada