3G2060(R)

Cellular Wireless Alarm Communicator

Cellular Communicator – North America

TL2603G(R)

Ethernet/Internet and Cellular Dual-Path Alarm Communicator

Cellular / Ethernet Communicator - North America

INSTALLATION MANUAL V3.0

Warning: This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer.

TABLE OF CONTENTS

General 1

Technical Specifications 2
UL/ULC Installation Requirements 2
Ratings Compatibility 4

Pre Installation Configuration 5
Encryption 5
Communicator Installation Configuration 5
Installing the Ethernet Cable 5
Running the RS-422 Cable 5
Inserting and Removing the SIM Card 6
Installing the Ethernet Cable 5
Installing Cellular/Ethernet Communicator in Panel 6
Communicator Placement Test 9
Initial Panel Programming 10
Communicator Status Leds 11
Communicator Reset / Update 13
Programming Options Sections
Ethernet/Cellular Programming Options 16
System Options 16
Programming Options 19
Communications Reporting Codes 20
Ethernet Receiver 1 Options 22
Ethernet Receiver 2 Options 23
Ethernet Options 24
Cellular Receiver 1 Options 24
Cellular Receiver 2 Options 25
Cellular Options 26
System Information (Read Only) 27
System Reset Defaults 28
Communicator Status, Initialization, Diagnostics and Troubleshooting 28
Programming Worksheets Sections
Ethernet/Cellular Programming Worksheets 32
System Options 32
Ethernet Receiver 1 Options 33
Ethernet Receiver 2 Options 33
Ethernet Options 33
Cellular Receiver 1 Options 33
Cellular Receiver 2 Options 33
Cellular Options 34
System Information (Read Only) 34
System Reset Defaults 34

Limited Warranty 35

WARNING: INSTALLER PLEASE READ CAREFULLY

Note to Installers

The Warnings on this page contain vital information. As the only individual in contact with system users, it is the installer's responsibility to bring each item in this Warning to the attention of all 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 the reasons may be:

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.

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.

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.

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 your security system be reviewed periodically to ensure that its features remain effective and that it is updated or replaced if it is found that it does not provide the protection expected.

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.

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.

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.

Insufficient Time

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

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, barbecues, fireplaces, sunlight, steam vents, lighting and so on.

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.

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 emergency situation.

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.

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.

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, other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

GENERAL

IMPORTANT

This installation manual shall be used in conjunction with the PowerSeries control panel. All the safety instructions specified within that manual shall be observed (or equivalent). The PowerSeries control panel is referenced as the "panel" throughout this document.

The Cellular/Ethernet Communicator is a fixed, wall-mounted unit, located inside the panel, and shall be installed in the location 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,
- Interference between power limited and non power limited wiring,
- Loosening of terminal connections, or
- Damage of conductor insulation.

WARNING: Never install this equipment during a lightning storm!

Safety Information

The Installer must instruct the System user on each of the following:

- Do 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 service persons only.
- Use authorized accessories only with this equipment.
- Do not stay close to the equipment during device operation.
- Do not touch the external antenna.

Model Information

3G2060R: Is a HSPA (3G) Cellular Alarm Communicator that sends alarm communication to Sur-Gard System I, II, III (SG-DRL3IP), and IV (SG-DRL4IP) central station receivers via a HSPA(3G)/GPRS digital cellular network.

TL2603GR: Is a Dual-path HSPA(3G) Ethernet Alarm Communicator that sends alarm communication to Sur-Gard System I, II, III, and IV central station receivers through Ethernet/Internet or a HSPA(3G)/GPRS digital cellular network.

The communicator can be used as either a backup or primary communicator. The communicator supports Internet Protocol (IP) transmission of panel and communicator events over Ethernet/Internet and/or HSPA/GPRS.

The cellular performance of the **3G2060R** or **TL2603GR** Communicator depends greatly on HSPA(3G)/GPRS network coverage in the local area. The unit should not be mounted in the final location without first performing the Communicator Placement Test below to determine the best location for radio reception (minimum of one green LED ON). Optional antenna kits are available from DSC at: **http://www.dsc.com**.

NOTE: Prior to installation of the 3G2060R or TL2603GR Communicator, confirm with your local service provider that the HSPA(3G)/GPRS network is available and active in the area where the communicator will be installed, and that radio signal strength (CSQ) is adequate.

Panel Mounting

The following communicators are compatible with PC1616/PC1832/PC1864 panels:

- **3G2060R**, **3G2060** (HSPA(3G)/GPRS only)
- **TL2603GR, TL2603G** (Ethernet/Internet + HSPA(3G)/GPRS dual-path)

NOTE: This manual covers communicator models with and without 'R' throughout entire manual unless specifically stated otherwise.

Features

- 128-bit AES encryption via cellular and ethernet/internet (NIST Validation Certificate No. 2032).
- Back up or primary cellular alarm communication.

- Automatically switches to 2G (EDGE/GPRS) if HSPA(3G) service is not available.
- Ethernet LAN/WAN 10/100 BaseT (TL2603GR only).
- Full event reporting to central station (UL/ULC listed) and C24 Interactive, via RS-422 to the C24-HUB ('R' models only). This supplementary feature is in addition to a UL/ULC Listed system configuration and it does not affect the required UL/ULC Listed signaling.
- Fully redundant Ethernet/Internet and cellular Dual-path Alarm Communication (TL2603GR only).
- Individual Ethernet and/or Cellular periodic test transmission.
- Interactive support via Gateway or Data over cellular network.
- Integrated call routing.
- Remote firmware upgrade capability of the communicator and panel firmware via Ethernet and/or cellular.
- Dual-Band Operation: 850 MHz, and 1900 MHz (North America only).
- Panel remote uploading/downloading support via cellular and Ethernet/Internet.
- PC-LINK connection.
- Programmable Labels.
- RS-422 balanced line for supplementary communication to the external C24-HUB up to 1,000 ft. (305 m) for C24 Interactive. (This supplementary feature is in addition to what is required for a UL/ULC listed system configuration and it does not affect the required UL/ULC listed signaling). Only models with "R".
- SIA and Contact ID (CID) formats supported.
- Signal strength and Trouble display LEDs.
- Subscriber Identity Module (SIM) card included with Communicator.
- Supervision heartbeats sent via cellular and Ethernet/Internet.

Technical Specifications

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

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

UL/ULC Installation Requirements

NOTE: For equipment used at the protected premises and intended to facilitate IP communications (hubs, routers, NIDs, Digital Subscriber Line (DSL), Cable modems), 24 hour back-up power is required. Where such cannot be facilitated, a secondary (back-up) communication channel is required.

Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems.

Notes for using Private, Corporate, and High Speed Data Networks:

Network access and domain access policies shall be set to restrict unauthorized network access, and spoofing or Denial of Service (DoS) attacks. Select an Internet Service Provider (ISP) that has redundant servers/systems, back-up power, routers with firewalls enabled, and methods to identify and protect against DoS attacks (e.g., via spoofing).

Notes for using Public Switched and Cellular Data Networks:

Communication channels shall be facilitated such that the communicator will restrict unauthorized access, which could otherwise compromise security. The communicator shall be located in a secured area.

- For **ULC Residential** Fire and Burglary applications the **TL2603GR** can be used as primary communication channel via either cellular or Ethernet or as a back-up in conjunction with the Digital Alarm Communicator Transmitter (DACT). Test transmission every 24 hours shall be enabled on each channel.
- For **ULC Commercial** Fire and Burglary applications the **3G2060R** and **TL2603GR** can be used as a passive communication module with the following Security Levels:
  - P1 (each channel cellular or Ethernet is independent)
  - P2 (cellular and Ethernet in back-up configuration, Panel Section **[851][005]** Toggle Option [5] OFF).
- P3 (cellular and Ethernet in redundant configuration, Panel Section **[851][005]** Toggle Option [5] ON).

- The Communicator can also be used as an Active communication system with the Security Levels A1-A4 (each channel cellular or Ethernet independent or together in a back-up/redundant configuration). For Active Line Security systems AES128 bit encryption shall be enabled (at the monitoring station receiver) and the supervision heartbeat rate shall be set as **90** seconds (Panel Section **[851][004]** = 005A/90). The supervision window at the Signal Receiver Center (SRC)'s receiver shall be programmed as maximum of **180** (00B4/180) seconds.
- For **UL Residential** Fire and Burglary applications the **3G2060R** and **TL2603GR** can be used as the primary communication channel via either cellular or Ethernet, or as a back-up in conjunction with the DACT
  (30 day test transmission is required on each channel).
- For **UL Commercial** Burglary applications the **TL2603GR** can be used as Dual Signalling Line communication system (cellular and Ethernet channels used in redundant configuration), Standard Line Security and as Encrypted Line Security.
- The supervision heartbeat shall be enabled (Panel Section **[851][005]** Toggle Option [1] (Ethernet) and/or Toggle Option [2] (cellular) shall be ON), Toggle Option [3] (Supervision Type) shall be ON and the supervision heartbeat rate shall be selected as **135** (0087/135) seconds. Option [004] = 0087. The supervision window at the supervising station shall be maximum **200** (00C8/200) seconds. For Encrypted Line Security systems the encryption AES128 bit shall be enabled at the monitoring station receiver.
- For **UL Commercial** Burglary installations, the **3G2060R** is listed as a primary (sole) communication means (heartbeat must be enabled) or for supplementary (back-up) use in conjunction with a Plain Old Telephone Service (POTS) line dialer. When the heartbeat transmission over the Ethernet or cellular network is enabled, using the **TL2603GR** with a compatible control unit listed for standard/encrypted line security, it can provide line security for the alarm system over the primary line.
- The **TL2603GR** is also suitable to be used with a compatible control unit listed for dual line security transmission when used in conjunction with a DACT or a Public Switched Data Network (PSDN) transmitter, where the PSDN provides the line security and is the primary line. In this mode, alarm signals are required to be sent simultaneously over both communication methods.
- For UL Residential Fire installations, a test transmission is sent to the Monitoring station every 7 days. This is the default setting in the product.

Ratings Compatibility

Table 1: Communicator Ratings

Model	3G2060R Cellular only	TL2603GR Ethernet and Cellular
Power Supply Ratings		
• Input Voltage	Nominal 12 VDC: The panel Bell output shall be derated: 700mA - (Communicator mA) = (derated Bell output).	
Current Consumption		
• Standby Current	90mA @ 13.66V	120mA @ 13.66V
• Alarm (Transmitting) Current	400mA @ 12V	
• Operating Frequency	850MHz, 1900MHz	
• Typical Antenna Gain	2dB**i**	
Environmental Specifications		
Operating Temperature	32°F - 120°F (0°C - 49°C)	
Humidity	5% ~ 93% relative humidity, non-condensing	
Mechanical Specifications		
Board Dimensions (mm)	100 × 150 × 15	100 × 150 × 15
Weight (grams) with bracket	310	320

Table 2: Compatible Receivers, and Panels

Communicator	Receiver/ Panel	Description
3G2060R	Receiver	• Sur-Gard System I Receiver, version 1.13+ • Sur-Gard System II Receiver, version 2.10+ • Sur-Gard SG-DRL3-IP, version 2.30+ (for Sur-Gard System III Receiver) • Sur-Gard SG-DRL4-IP version 1.20+ (for Sur-Gard System IV Receiver)
TL2603GR	Panel	• Power Series PC1616, version 4.5+ • Power Series PC1832, version 4.5+ • Power Series PC1864, version 4.5+

NOTE: Enter [*][8][Installer Code][900] at keypad to view the Panel Version number.

Products or components of products, which perform communications functions only shall comply with the requirements applicable to communications equipment as specified in UL60950 or CAN CSA C22.2. No. 60950-1, Information Technology Equipment - Safety - Part 1: General Requirements. Where network interfaces are internal to the control unit or receiver, compliance to CAN CSA C22.2. No. 60950-1 is adequate. Such components include, but are not limited to: hubs; routers; NIDs; third-party communications service providers; DSL modems; and Cable modems.

C24 Interactive

NOTE: This application has not been investigated by UL/ULC and is not be used on UL/ULC certified installations.

The Communicator provides C24 Interactive monitoring and control via an RS-422 interface to an external C24-HUB. The default Keybus link speed is 115.2 KB and this option is programmable by the installer. All life-style events are transmitted by the RS-422 link to the C24-HUB and then remotely to the C24 Interactive Servers.

NOTE: The C24-HUB is an interface device which connects to security panels, IP cameras, sensors, Z-wave based home automation devices, etc. to deliver a host of advanced functionality.

NOTE: Life-style events are “non alarm” events. Life-safety events are “alarm” events.

The following features are available with the RS-422 C24 Interactive:

- Communicator faults can be transmitted.
- Panel communication errors are reported to the C24-HUB.
- Real time reporting of Zone status information to the C24 Interactive Server.
- Remote update of the Communicator (flash upgrade).
- SMS incoming “wake up” for the cellular channel.
- WEB login to request an incoming session with the Communicator.
- Zone Label Programming.

NOTE: Communicator buffers 1000 date/time stamped Life-Style events to the C24-HUB as First In First Out (FIFO).

NOTE: When Interactive is enabled, (Via Gateway or Data Network) Upon exiting installer programming, communicator will synchronize programming with control panel. This process takes approx. 5 seconds, during this time the keypad will be "Function Not Available".

PRE INSTALLATION CONFIGURATION

Encryption

The Communicator uses 128 Bit AES Encryption. Encryption can only be enabled from the monitoring station receiver. Each receiver (Ethernet 1 and 2, cellular 1 and 2) can independently have encryption enabled or disabled. When encryption is enabled, the central station will configure the device to encrypt communications the next time the Communicator module performs a communication to that receiver.

NOTE: Packets will start being encrypted only after the next event is sent to that receiver, or if the unit is restarted.

Before leaving the installation site, the Communicator TL2603GR Ethernet line shall be connected via an APPROVED (acceptable to the local authorities) Network Interface Device (NID) (e.g., for UL Installations, UL60950 listed NID). All wiring shall be performed according to the local electrical codes.

COMMUNICATOR INSTALLATION CONFIGURATION

This Cellular/Ethernet Communicator 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 to in performing a task and can also take measures to minimize the risks to that person or other persons). The Communicator shall be installed and used within an environment that provides the pollution degree max 2, overvoltages category II, in non-hazardous, indoor locations only. This manual shall be used with the Installation Manual of the panel which is connected to the Cellular/Ethernet Communicator. All instructions specified within the panel manual must be observed.

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

Installing the Ethernet Cable

TL2603GR only

A Category 5 (CAT 5) ethernet cable must be run from a source with Ethernet/Internet connectivity to the Communicator module, inside the Panel. The Communicator end of the cable must be terminated with an RJ45 plug, which will connect to the Communicator's RJ45 jack after the Communicator is installed. All requirements for installation of CAT5 ethernet cable must be observed for correct operation of the Communicator, including, but not limited to, the following:

- Do NOT strip off cable sheathing more than required for proper termination.
- Do NOT kink/knot cable.
- Do NOT crush cable with cable ties.
- Do NOT untwist CAT5 pairs more than ½ in. (1.2cm).
- Do NOT splice cable.
- Do NOT bend cable at right angles or make any other sharp bends.

NOTE: CAT5 specification requires that any cable bend must have a minimum 2 in. (5 cm) bend radius. Maximum length of CAT 5 cable is 328 ft. (100 m).

Running the RS-422 Cable

An RS-422 cable must be connected to the C24-HUB and cable run to the Communicator module inside the panel.

NOTE: Maximum cable length for RS-422 cable is 1,000 ft. (305 m).

At the **C24-HUB**, make connections as follows:

1. Securely fasten the **TX+** wire on the terminal block.
2. Securely fasten the **TX-** wire on the terminal block.

3. Install a **120 Ω¼ W** resistor between the **RX +** and **RX-** terminals at the C24-HUB.
4. Securely fasten the **RX+** wire on the terminal block.
5. Securely fasten the **RX-** wire on the terminal block.
6. (Optional) Securely fasten the **GND** wire on the terminal block.

NOTE: The GND connection is optional. DSC recommends connecting the GND wire at both ends.

7. Run the RS-422 Cable from the C24-HUB to the inside of the Panel.

Inserting and Removing the SIM Card

1. Remove the front cover of the Panel to access SIM holder.
2. Remove power from the panel and disconnect the battery and telephone line.
3. On the SIM card holder push gently to slide the cover towards the Printed Circuit Board (PCB) antenna, as indicated by the arrow on SIM holder, to **OPEN**. This will unlatch the SIM card holder on the side closest to edge of the Communicator PCB. (See **Figure 3**).
4. Lift up the SIM card holder from the side that is not hinged.

NOTE: The SIM can be damaged by bending, or scratching contacts. Use caution when handling SIM cards.

5. Insert or remove the SIM card, noting the orientation of the notches on the SIM card and the SIM card holder.
6. When inserting a SIM card, insert the card in the proper orientation and gently push the SIM card holder down and slide the holder as indicated by the arrow on SIM holder, to **LOCK**.
7. Reconnect the backup battery and telephone line, apply AC power to panel, and replace the panel cover.

Hardware Reset

The Communicator can be hardware reset by installing a jumper between Pins 4 and 5 on the AUDIO/DEFAULT connector and restarting the Communicator. Installing jumper during normal operation has no effect.

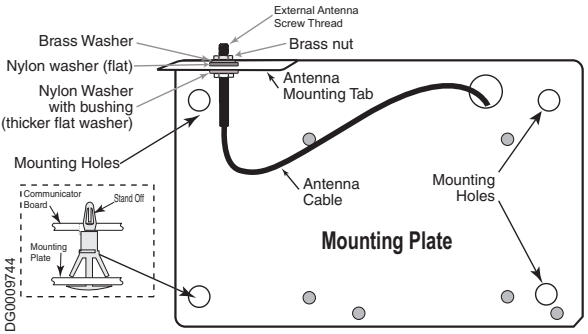
Installing Cellular/Ethernet Communicator in Panel

Installing Communicator with PC1616/1832/1864 Panel

NOTE: Before installing Communicator or inserting/removing SIM, ensure that system power is OFF and telephone line is disconnected.

1. To assemble supplied mounting bracket, perform the following: (See **Figure 1**).
   a. Remove the 4 white plastic standoffs from the bag provided with the Communicator kit.
   b. Insert the 4 standoffs through the back of the mounting bracket, into the holes at each corner. (The antenna mounting tab should be facing away from you).
   c. Place the bracket on a flat, solid surface. Hold the Communicator component side up and orient the 4 holes on the Communicator with the 4 standoffs protruding from the bracket. Push the Communi-

Figure 1:Communicator Mounting Bracket



cator firmly and evenly onto the standoffs until it is securely attached to the mounting bracket.

d. Remove the panel front cover.

e. Remove and discard the circular knockout located in the top-right section of the panel. (This hole will be used for connection of the supplied radio antenna).

f. Connect the supplied 5" (12.7 cm) antenna cable to the radio, by passing the connector through the hole on back of the mounting bracket to the communicator board. Push the antenna connector firmly into the socket on the cellular radio. (See **Figure 3**).

2. Install the Communicator into the panel:

a. Attach one end of the PC-LINK cable to the panel PC-LINK header on the panel (red wire goes on Pin 1 of the **panel** PC-LINK header).

b. Insert the assembled Communicator into the panel.

NOTE: Ensure that the threaded antenna connection point is visible through the knockout hole at the top right of the panel.

c. Place the nylon washer with bushing (thick flat washer) onto the threaded section of the antenna cable. Insert the threaded section through the antenna mounting knockout hole at top right of panel.

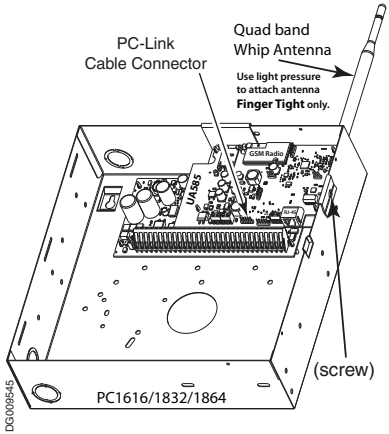
d. Place the second nylon washer (flat), followed by the brass washer and the brass nut, onto the threaded section of the cable, **outside** the panel. Tighten the assembly by hand only. (Finger tight only- Do not overtighten the antenna assembly).

e. Locate the screw hole on the right side wall of the panel. See **Figure 2** (screw). Line up the assembled Communicator with the right side wall of the panel and, using the screw provided, secure the mounting bracket to the panel.

f. Attach the other end of the PC-LINK cable to the Communicator (black wire goes on Pin 1 of the **Communicator).**

g. Using light pressure (finger tight only), attach the supplied white quad band whip antenna to the threaded antenna connection point at top of the panel.

Figure 2:PC1616/1832/1864 Control Panel



WARNING! - 3G2060R/TL2603GR modules are power limited. Do not route any wiring over the circuit board. Maintain at least 1in. (25.4mm) separation between circuit board and wiring. A minimum of ¼ in. (7mm) separation must be maintained at all points between non-power limited wiring and power limited wiring.

3. To electrically connect the Communicator to the panel, perform the following steps (See **Figure 3).**

a. Disconnect both AC power and battery connections from the panel, and disconnect telephone line.

Module Power Connection

b. Attach a wire from the Communicator's left **PWR** terminal to the panel's **BELL+** terminal.

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

c. Attach a wire from the Communicator's **GND** terminal (beside PWR) to the panel's **AUX -** terminal.

d. Attach a wire from the Communicator's **SHLD** terminal to the panel's **EGND** terminal. (Protective earth ground).

(Optional) External Bell/Siren Connection

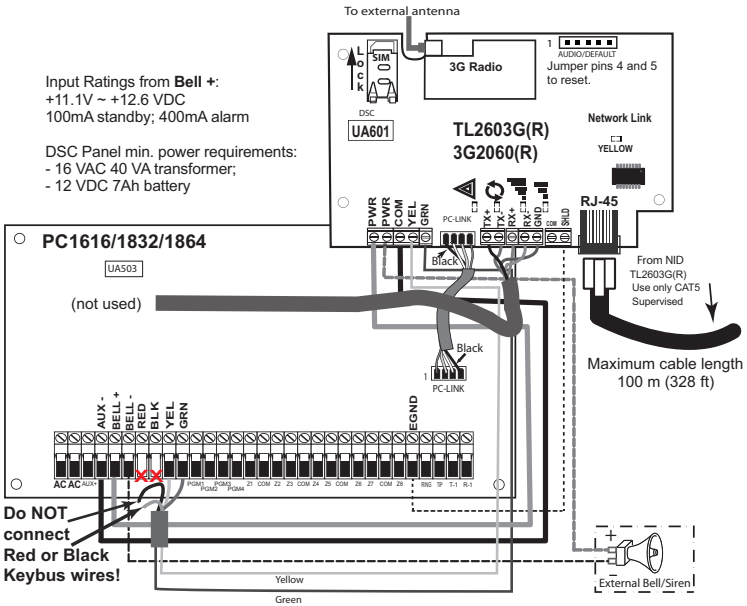
e. Attach a wire from the Communicator's right **PWR** terminal to the positive (+) terminal on the Bell/Siren.

f. Attach the panel's **BELL –** terminal to the negative (**–**) terminal on the Bell/Siren.

NOTE: If an external Bell/Siren is not used, install the 1KΩ½W 5% resistor (Brown, Black, Red, Gold) (supplied with the panel) between the panel's Bell + and Bell – terminals, then only wire the BELL + to the PWR terminal on the Communicator.

g. Confirm that the SIM card is inserted in the holder and locked.

Figure 3:Communicator Wiring Diagram



Keybus Connection for C24 Interactive

4. Install the Keybus cable between Communicator and Panel as follows:
   WARNING: DO NOT CONNECT KEYBUS **RED** OR **BLK** WIRES TO THE PANEL OR THE COMMUNICATOR TERMINAL BLOCKS.
   a. Attach a wire from the Communicator **YEL** terminal to the panel **YEL** terminal.
   b. Attach a wire from the Communicator **GRN** terminal to the panel **GRN** terminal.

RS-422 Connection for C24 Interactive

At the Communicator inside the Panel, connect the previously run RS-422 cable as follows:

1. Securely fasten the **TX+** wire to **RX+** on the terminal block.
2. Securely fasten the **TX-** wire to **RX-** on the terminal block.
3. Securely fasten the **RX+** wire to **TX+** on the terminal block.
4. Securely fasten the **RX-** wire to **TX-** on the terminal block.
5. (Optional) Securely fasten the **GND** wire on the terminal block.

NOTE: The GND connection is optional. DSC recommends connecting GND wire at both ends.

Install Network Cable (TL2603GR only)

6. Route the CAT 5 Ethernet cable through back of the panel and plug it into the Communicator's RJ45 jack.

NOTE: Before leaving the premises the Ethernet communication lines must first be connected to an approved (acceptable to local authorities) type NID, (UL installations, UL 60950 listed NID, for ULC installations CAN/CSA C22.2. No. 60950-1 Certified NID). All wiring shall be performed according to the local electrical codes.

7. Perform the following steps for initial power on of the panel with Communicator installed:

a. Reconnect the AC power, telephone line, and battery + connector to the panel. (The Communicator and Panel will power up together).
b. Observe that the Communicator's red and yellow LEDs are flashing together while it initializes. The red and yellow LEDs will continue to flash until the Communicator has successfully communicated to all programmed receivers. If this is the first time the Communicator has been powered up in the panel, the module will initiate communication to Connect24 to request remote programming.

NOTE: Initialization may take several minutes to complete. red and yellow LEDs will flash together during initialization. Do not continue to next step until the red and yellow LEDs have stopped flashing. (If only the yellow LED is flashing, there is a Communicator trouble and the Green LEDs are not valid for Communicator Placement Test). Correct trouble indicated by flashes on yellow LED before continuing. (See Table 5 for troubleshooting assistance).

8. Perform the Communicator Placement Test below.
9. Mount the Panel in final location indicated by placement test.

COMMUNICATOR PLACEMENT TEST

3G2060R and TL2603GR only

To confirm that the cellular antenna location is suitable for radio operation, perform the placement test as follows:

NOTE: You may need to relocate the Panel or install an optional extension antenna during this procedure, if radio signal strength is too low.

1. Confirm that the yellow LED on the Communicator is not flashing. A flashing yellow LED indicates trouble on the Communicator. See Table 5 to troubleshoot and correct the cause of this trouble before continuing to the next step.
2. Observe the strength of the radio signal on the yellow LED and the 2 green LEDs on the Communicator meet or exceed the minimum signal level requirement. Minimum Signal Level: The yellow LED is **OFF** and the Green LED 1 (furthest from the yellow LED) is **ON**. (i.e., not flashing) for the panel location to be acceptable. See table for **"Radio Signal Strength" on page 13** for interpretation of receiver signal strength on LEDs.

NOTE: If the required signal strength is too low with the panel in its current location, the panel must be relocated or an external antenna is required.

a. If required, the following cellular extension antenna kits are available to the installer:

- GS-15ANTQ - 4.57m (15') Internal Antenna Extension Kit *(*Suitable for interior mounting only*).*
- GS-25ANTQ - 7.62m (25') External Antenna Extension Kit *(*Suitable for exterior mounting only*).*
- GS-50ANTQ - 15.24m (50')External Antenna Extension Kit *(*Suitable for exterior mounting only*).*

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

3. If required, install the antenna extension and perform the following steps to determine the best location for placement of the antenna :
   a. Disconnect the white whip antenna from the panel.
   b. Attach one end of the antenna extension cable to the threaded antenna connector on the panel and the other end to the external antenna.
4. Move the extension antenna to various locations while observing the two Green LEDs on the panel.
   a. Continue to reposition the extension antenna until you receive an acceptable (minimum one green LED ON solid) signal strength.

NOTE: Minimum strength is: green LED 1 flashing and yellow LED OFF. If green LED 1 is flashing, relocation should be considered.

b. Mount the supplied antenna extension bracket at the location that provides the best signal strength.

5. Alternately, you can reposition the Panel to improve signal strength. Dismount the panel and move it to another location to achieve the required signal strength. If the Panel is relocated to improve signal strength, mount it in the new location.
6. When final Panel/antenna location is determined, continue at the **Initial Panel Programming**-section.

INITIAL PANEL PROGRAMMING

Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems.

Keypad Data Display

NOTE: Programming locations accessible via the keypad are for viewing only. All communicator programming is modified via Connect24.

- **Section-Toggle Options:** The number is displayed when Toggle is ON, the number is not displayed when Toggle is OFF. (e.g., Toggle Options displays: [--3--6--]. Options **3** and **6** are **ON**, all others are **OFF**). Pressing keys 1 through 8 will alternately turn the Toggle ON and OFF.
- **HEX/Decimal Data**: Values that are provided with two defaults, separated by a "/" character, use the format: hexadecimal followed by decimal equivalent (e.g., Default [0BF5/3061]). Hexadecimal numbers are shown, with all leading zeroes, to the full field length defined for the number.

Entering HEX values at keypad

To enter HEX values at the keypad, you must press the ***** key before entering the HEX value. (e.g., to enter "**C**" at the keypad, press **[*][3]**.

Entering ASCII Characters at keypad

1. Press [*] and use scroll buttons **[<] [>]** to display "ASCII Entry" on the LCD screen.
2. Press [*] to select ASCII entry mode.
3. Use the **[<] [>]** scroll keys to display the character you want and press [*] to save and exit ASCII.
4. Repeat the steps above to enter another ASCII character.

PC1616/1832/1864 Initial Programming

Perform the following steps to ensure that the Communicator and the Panel work together as intended.

These Sections must be programmed at the panel keypad. Enter **[*][8][Installer Code][Section Number]**. Record any values that are modified from their default, in the appropriate Worksheets for the Panel or Communicator.

1. In Panel Section [**167**] program **060** (seconds).
2. In **Panel** Section [**382**] set Option [**5**] ON

NOTE: If this option is OFF, the yellow status LED on the Communicator will indicate 'Panel Supervision Trouble' (2 flashes) and the unit can not be programmed via the PC-LINK cable.

NOTE: Account Number in Communicator Section [851][021] automatically syncs with Panel Section [310] for Panel Versions 4.50 or newer

3. A valid Account Number must be entered in Communicator Section **[851][021]**. See Programming Section.

NOTE: DSC recommends using the same Account Number for Panel and Communicator.

4. In Panel Sections [301], [302], and [303], program the central station telephone number that will be used for the cellular/Ethernet Communicator. Valid entries are:
   a. A valid telephone number; signals will be routed to the central station using the PSTN.
   b. **DCAA** (Receiver 0); signals will be routed to cellular/Ethernet Receivers 1 - 4 depending on programming Toggle Options in Communicator Section [851][006].
   c. Panel Section [301] sets the Primary communication path, and may be configured as either PSTN or Communicator routing. Panel Section [302] is redundant, and Panel Section [303] is the backup telephone number for Panel Section [301]. Refer to the Panel manual for additional information.

NOTE: The leading digit 'D' (dial tone detection) in the telephone number is pre-programmed.

5. In Panel Section [350], program the communication format as: CID (03) or SIA FSK (04).
6. In Panel Sections [351] - [376], program the Communicator call direction options. Refer to the Panel Installation Manual for details on setting these options.
7. In Panel Section [401] set Toggle Option [2] 'User Enable DLS' to **ON** in order to perform panel DLS session through cellular or Ethernet.

NOTE: Before leaving the premises, the installer should verify all programmed communications paths. See Programming Options Section [851][901] to send immediate test transmissions.

NOTE: Sending Test Transmissions to Receivers that are Not Programmed will generate FTC Trouble.

Communicator Troubles displayed on a PC1616/1832/1864

The General System trouble is the only trouble that will appear on the keypad Liquid Crystal Display (LCD) when encountered by a Communicator installed in a PC1616/1832/1864. For more information about the trouble on the Communicator module refer to the panel event buffer. Log entry will show Fault or Restore for each of the following events:

- **T-LINK Network Fault/Restore**: This log will occur for the following trouble conditions: SIM Lock Trouble, cellular Trouble, Ethernet Trouble, or Connect24 Configuration Trouble.
- **T-LINK Receiver Trouble/Restore**: This log will occur for the following trouble conditions: Receiver Not Available Trouble, Receiver Supervision Trouble, or Failure to Communicate (FTC) Trouble.
- **T-LINK Comm. Fault/Restore**: This log will occur when the panel loses communications with the Communicator and will clear when communications is restored.

COMMUNICATOR STATUS LEDS

The Communicator has 4 on-board LED indicators. These include 1 yellow trouble LED, 1 red Network Connection Status LED, and 2 green Signal Strength LEDs. The LED meaning is described in this Section.

⚠Yellow Trouble 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 coded flashes and the conditions which will activate the Trouble Status LED.

Table 3: Yellow Trouble Status LED

# of Flashes	Trouble	# of Flashes	Trouble
2	Panel Supervision Trouble	8	Receiver Supervision Trouble
4	SIM Lock Trouble	9	FTC Trouble
5	Cellular Trouble	10	Configuration Failure
6	Ethernet Trouble	11	Remote Programming
7	Receiver Not Available Trouble	12	Module Configuration Trouble

NOTE: Only the highest priority trouble (2 Flashes is the highest priority trouble) is indicated. When this trouble is restored, the next highest trouble will indicate, if present. This will continue until all troubles have been cleared. (yellow LED is not flashing).

The following paragraphs describe the conditions associated with the trouble indicated:

Panel Supervision Trouble (2 Flashes)

This trouble will be indicated when communication between the Communicator module and the Panel fails. If the module can not communicate with the Panel (e.g., loss of power to the panel) the Communicator will send the 'Panel Absent Trouble Event' message to the central station receiver. When communication returns, a 'Panel Absent Restore Event' is sent by the Communicator to the central station receiver. The reporting codes are ET001 for Trouble and ER001 for Restore. The panel absent event always uses the primary receiver account code when communicating to the central station.

NOTE: The Panel Supervision Trouble/Restore are internally generated events by the Communicator. Trouble is generated if the Communicator misses 6 Polls. Trouble is restored on receipt of first Poll from the Panel.

SIM Lock Trouble (4 Flashes)

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.

Cellular Trouble (5 Flashes)

This trouble is indicated for any of the following 4 conditions:

1. **Radio Failure**: Trouble is indicated after 8 failed attempts to communicate with the cellular radio.
2. **SIM Failure:** Trouble is indicated after 10 failed attempts to communicate with the SIM.
3. **Cellular Network Trouble**: Trouble is indicated for loss of the registration to the network provider.
4. **Insufficient Signal Strength**: Trouble is indicated if **calculated average** signal strength is too low. (Both green LEDs are OFF). Trouble will clear when the calculated average signal strength is above minimum (i.e., > CSQ 5).

NOTE: If Option [851][006] Bit 8 is Off, CSQ ≥ 4 will not trigger Cellular Trouble

Ethernet Trouble (6 Flashes)

This trouble is indicated when Ethernet link between the transmitter and the local switch or router is absent. This trouble will also be indicated if the unit fails to get Dynamic Host Control Protocol (DHCP) settings from the DHCP server. (Not active if Ethernet Receivers are not programmed).

Receiver Not Available (7 Flashes)

This trouble is indicated if the unit is not able to successfully initialize with any of the programmed receivers. Unprogrammed receivers are excluded. This trouble is also indicated if the cellular receiver APNs have not been programmed in Sections [205] and [215].

Receiver Supervision Trouble (8 Flashes)

This trouble is indicated when receiver supervision is enabled and communication between the Communicator module and the receiver fails. Trouble is indicated if Ethernet 1 and/or Cellular 1 is supervised and does not receive a heartbeat from the receiver or if cellular is supervised and the unit does not receive an acknowledgment to 4 heartbeats sent to the receiver.

FTC Trouble (9 Flashes)

This trouble is indicated when the unit fails to communicate module events to the central station. Trouble is displayed after the unit has exhausted all communications attempts to all programmed receivers for events generated by the Communicator.

Configuration Failure (10 Flashes)

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

Remote Programming (11 Flashes)

This trouble indicates that a remote firmware update is in progress over the cellular/ethernet network. The Trouble will clear automatically when the update is completed successfully.

Module Configuration Trouble (12 Flashes)

This trouble is indicated when the System Account Code or the Receiver Account have not been programmed. Disabled receivers are excluded.

⚠ Red Network Connection Status LED

TL2603GR

BLINKING: Indicates communications in progress.

- Once quickly for outgoing Ethernet transmission.
- Twice quickly to indicate incoming Ethernet ACK/NACK.

OFF: This is the normal state of the Red Network Connection Status LED. There are no network connection issues present.

ON: There is a problem with the Ethernet or the cellular network connection. LED will be ON if any of the following occur:

- Ethernet cable is not connected,
- DHCP configuration times out,

- Unit fails to get an IP address from the cellular network, or
- Cellular connection has been reset.

(Green LED 1) (Green LED 2) and (Yellow LED) Signal Strength

NOTE: If the yellow LED is flashing, Signal Strength in table below is not valid. See **Table 5** for troubleshooting flashing yellow LED.

Table 4: Radio Signal Strength

Signal Strength	CSQ Level	Yellow LED	Green Led 2	Green LED 1	Signal Level dBm	Action Required
No Signal	0	ON	OFF	OFF	-108.8	Check all antenna connections. Confirm cellular service is active in area. Relocate Panel or install external antenna.
1 Bar	1 - 4	ON See Note	OFF	Flashing	-108 ~ -103	Relocate Panel or install external antenna if Yellow Trouble LED has: **5 flashes**.
2 Bars	5 - 6	OFF	OFF	Flashing	-102 ~ -99	
3 Bars	7 - 10	OFF	OFF	ON	-98 ~ -91	**Location is OK**. Cellular signal strength is greater than CSQ 7.
4 Bars	11-13	OFF	Flashing	ON	-90 ~ -85	
5 Bars	14 +	OFF	ON	ON	-84 and higher	

NOTE: The communicator will indicate cellular Trouble (yellow LED = 5 flashes) if the calculated average CSQ Level is 4 or less. The communicator signal strength can be viewed remotely with Connect24.

Network Activity LEDs (Red and Green)

TL2603GR only

- **Ethernet Activity:** Red LED will blink quickly once for Transmit, or twice for Receive.
- **Cellular Activity:** Green LED 2 will blink quickly once for Transmit, or twice for Receive

COMMUNICATOR RESET / UPDATE

Factory Defaults Reset

You can reset the programming options for the Communicator to the factory settings by installing the hardware jumper. Perform the following steps to reset the Communicator:

NOTE: A jumper is required on AUDIO/DEFAULT pins 4 and 5 to reset the hardware values.

1. Remove panel front cover.
2. Locate the AUDIO/DEFAULT 5 pin connector on the communicator board (see Figure 3).
3. Apply a jumper to short the hardware default pins 4 and 5.
4. Remove AC and DC power from the panel and then reapply power to the Panel. Wait until the two green LEDs on the communicator begin flashing rapidly.
5. Remove the jumper from the hardware default pins 4 and 5 (Green LEDs will stop flashing).
6. Replace the panel cover.

NOTE: The communicator has now been reset to the factory default values.

Firmware Update

The firmware of the device can be updated over cellular or Ethernet (Remote or Local updating):

- When the firmware update begins, all 4 LEDs are ON.
- During the firmware update process, the LEDs will be cycled individually in a chaser pattern.
- During the firmware update process, Chaser pattern will briefly pause, and resume again. This indicates Firmware Verification check has passed, and Application Update will begin.
- After a successful update, the unit will automatically restart.
- Should the update fail, all 4 LEDs will flash ON, then OFF together at 1 second intervals.

NOTE: If the firmware update fails, restart the Communicator by cycling Power. For persistent update failures, contact your dealer. For UL/ULC listed installations, only local firmware updates are allowed.

COMMUNICATOR TROUBLESHOOTING

NOTE: For additional details:

- Refer to Section [983] for troubleshooting the firmware updates
- Refer to Section [984] to verify the trouble status
- Refer to Section [985] for troubleshooting Connect24 programming

Table 5: Trouble LED indications

Trouble indication	Possible Causes	Trouble Possible Solution
No Indication	No Power	• Check the power connections between the Panel and the Communicator. • Confirm PC-LINK cable is properly installed between communicator and panel.
Yellow LED – ON Solid	Insufficient Signal Strength	• Confirm that cellular network service is active in your area. • Ensure the antenna is securely connected to the radio. Check antenna stub cable is securely connected to the radio. • If an external antenna is used ensure the antenna is securely screwed on to the antenna cable connector. Check external antenna for damage or open/short.
Trouble LED – 2 Flashes	Panel Supervision Trouble	• Check Section [382]Toggle Option[5] is ON.(cellular/Ethernet Module Enabled) • Ensure the PC-LINK cable between the Panel and Communicator is connected properly (not reversed) and is securely in place.
Yellow LED - 4 Flashes	Lockout Trouble	• The SIM card has incorrect PIN programmed or has a PIN that the module does not recognize. Replace the SIM card.
Yellow LED – 5 Flashes	Cellular Trouble	• Confirm that cellular service is available and active in your area. • Check all antenna connections. • Ensure **average** radio signal strength is CSQ **5** or higher. (See Table 4). • Ensure the SIM card is properly inserted into the SIM card holder. • Ensure the SIM card has been activated. (Could take up to 24 hrs after install). • If this trouble persists, you must relocate the Panel (and Communicator) or install an external antenna extension kit.
Yellow LED – 6 Flashes	Ethernet Trouble	• Check with your ISP to confirm Internet service is active in your area. • Ensure your Ethernet cable is securely inserted into the RJ45 jack of the Communicator and the Hub/Router/ Switch. • Check the link light on the Hub/Router/ Switch is ON . If link light is OFF, try restarting the Hub/Router/ Switch. • If DHCP is used, ensure that the unit has an assigned IP address from the server. In Section [851] [992] verify a valid IP address is programmed. If not, contact the Network administrator. • If problem persists, replace the Ethernet cable and RJ45 connector.
Yellow LED – 7 Flashes	Receiver Not Available	• Ensure that the Ethernet path has internet connectivity. • If you are using a static IP address make sure the gateway and subnet mask are entered correctly. • 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 for DHCP or have the proper IP address and port number. • Ensure the cellular receiver APNs have been programmed with the Access Point Name provided by your cellular provider.
Yellow 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.
Yellow LED - 9 Flashes	FTC Trouble	• The unit has exhausted all communications attempts to all programmed receiver for events generated by the Communicator. • Restart the system, if trouble persists, contact your dealer.
Yellow LED – 10 Flashes	Connect24 Configuration Failure	• The SIM is active but there is no programming for the Communicator. • Ensure a profile has been programmed in Connect 24 for the SIM. • You can confirm your programming by calling the Connect 24 VRU, or by logging into the Connect24 VRU web site.
Yellow LED – 11 Flashes	Remote Programming	• The LEDs will flash when a remote firmware upgrade is in progress over Ethernet or cellular. The LEDs will extinguish when update is complete.
Yellow LED – 12 Flashes	Module Configuration Trouble	• This indication appears when Section [021] System Account Code or Section [101]; [111]; [201]; and [211] Receiver Account Code have not been programmed. Ensure that a valid account code has been entered in these Sections.
All LEDs flashing together	Boot Loader Failed	• Disconnect power, then reconnect power to the Communicator module.
Red and Yellow LEDs flashing together	Initialization Sequence	• The unit is still initializing please wait while the unit gets its programming and establishes a connection to all programmed receivers. **Note: This process may take several minutes to complete.**
Only Green LEDs flashing	Hardware Default Jumper	• The hardware default jumper is installed and must be removed. See Figure 3.

ETHERNET/CELLULAR PROGRAMMING OPTIONS

The Programming Sections described in this document can be viewed at the keypad LCD. To start programming enter: **[*][8][installer code] [851][###]**, Where ### is the 3 digit section number referenced in this section. The Programming Worksheets at the end of this document can be used to record the new values when programming changes have been made from the default values.

Programming Sections are accessed through Connect24. Installers may **review/record** programming Options at the panel keypad.

NOTE: Ethernet/Cellular Programming Sections accessed through the panel are for **display purposes only**. Configuration changes must be done using Connect24.

NOTE: The Keypad is unable to view any sections that uses ASCII Characters

System Options

[001] Ethernet IP Address

Default (000.000.000.000)

Enter the IP address of the Communicator. Ensure that the IP address is unique to your Communicator on the local network. Format is 4 fields, each field is a 3 digit decimal number. Valid range: 000-255. If an IP address is programmed in this Section, the unit will operate with Static IP (DHCP disabled). Sections [002] and [003] must also be programmed when using Static IP addresses.

NOTE: Default for this Section is Dynamic Host Configuration Protocol (DHCP) enabled. When enabled, the DHCP Server will set values for: IP Address [001], Subnet Mask [002], and Gateway [003]. Programming an IP address in this Section will disable DHCP (Static IP).

[002] Ethernet IP Subnet Mask

Default (255.255.255.000)

Enter the Ethernet IP Subnet Mask of the Communicator. Format is 4 fields, each field is 3 digits. Valid range: 000-255.

NOTE: If DHCP is enabled, the DHCP Server will assign the subnet mask for this Section and the programmed value will be ignored.

[003] Ethernet Gateway IP Address

Default (000.000.000.000)

Enter the Ethernet Gateway IP address of the Communicator. The gateway IP address is required when a router is used on the local network to reach the destination IP address specified in Section [001]. Format is 4 fields, each field is a 3 digit decimal number. Valid range: 000-255.

NOTE: If DHCP is enabled, the DHCP Server will assign the Gateway IP address for this Section and the programmed value will be ignored.

[004] Receiver Supervision Interval

Default (0087/135)

When receiver supervision is enabled (ON) in Section [005] Toggle Option [3], the unit sends heartbeats to Ethernet Receiver 1 or Cellular Receiver 1 to test the communications path. Use this Section to set the interval time (in seconds) when heartbeats will be sent to the receivers. Valid range 000A-FFFF seconds. If the programmed value is less than (000A/10) seconds, supervision is disabled.

- **Receiver Window:** This is the supervision timeout that must be configured at the central station receiver.
- **Recommended Values:** This is the recommended heartbeat interval that should be programmed into the Communicator.
- For ULC installations, the Daily test transmission must be enabled over each available communication channel Sections [125] and [225]. When programming with Connect24, the recommended intervals will be programmed automatically when the required window is selected.

Table 6: Supervision Intervals for UL/ULC

Jurisdiction	Receiver Window (Timeout)	Recommended Supervision Interval
UL Commercial Burglary	200 seconds	(0087/135) seconds
UL Residential Fire	30 days	Panel Test Transmission
UL Residential Burglary	30 days	Panel Test Transmission
UL Commercial Burglary Active	180 seconds	(005A/90) seconds
UL Commercial Burglary Passive	24 hours	Panel Test Transmission
UL Commercial Burglary Fire Active	180 seconds	(0073/115) seconds
UL Commercial Burglary Fire Passive	24 hours	Panel Test Transmission

[005] System Toggle Options

[1] Ethernet Receiver 1 Supervised

Default (OFF)

TL2603GR only

ON: Ethernet Receiver 1 will be supervised and heartbeats will be sent to Ethernet Receiver 1 based on the supervision interval programmed in Section [004].

OFF: Ethernet Receiver 1 will not be supervised. When disabled, heartbeat 1 is sent to the Ethernet receiver once every hour, regardless of supervision type (heartbeat 1 or 2). The heartbeat is resent every 5 seconds until ACK. If no event or heartbeat ACK is received after (Receiver Supervision Interval + 75 seconds), Supervisory trouble is indicated.

NOTE: Ethernet Receiver 2 can not be supervised.

[2] Cellular Receiver 1 Supervised

Default (OFF)

ON: Cellular Receiver 1 will be supervised and heartbeats will be sent to Cellular Receiver 1 based on the supervision interval programmed in Section [004]. If ACK to heartbeat is not received, it is retransmitted every 5 seconds. Failure to ACK 2 consecutive heartbeats will reset the radio.

OFF: Cellular Receiver 1 will not be supervised. When disabled, heartbeat is not sent to the receiver. Supervisory trouble is indicated.

NOTE: Cellular Receiver 2 can not be supervised.

[3] Supervision Type

Default (OFF)

ON: Heartbeat 1 (Commercial Supervision). This supervision type is suitable for applications where swap detection is required on the supervisory packet.

OFF: Heartbeat 2 (Residential Supervision). This supervision type is suitable for applications where supervision of the communication path to the receiver is required. (no swap detection).

NOTE: Commercial supervision is more data intensive than residential supervision and should only be used when required to meet the approval for the installation.

[4] Primary Path

Default (OFF - **TL2603GR**) (ON - **3G2060R**)

ON: Cellular channel is the primary path. Ethernet channel is the secondary path, if it exists.

OFF: Ethernet channel is the primary path in a dual Communicator. Cellular channel is the secondary path.

[5] Redundant Communications

ON: Events will be communicated to Ethernet Receiver 1 and Cellular Receiver 1 at the same time. Events will be communicated to Ethernet Receiver 2 and Cellular Receiver 2 at the same time. As long as the event is successfully communicated to 1 of the 2 paths (Ethernet or Cellular) the Communicator will move on to the next event.

NOTE: Do not configure Ethernet Receiver 1 and Cellular Receiver 1 to communicate using a common receiver configuration (i.e., identical Receiver IP address and Receiver Remote Port).

OFF: Events will be communicated to the receivers individually.Toggle should be OFF when guaranteed message delivery to both receivers is required.

[6] Remote Firmware Upgrade

Default (ON)

ON: The Communicator module firmware can be remotely upgraded using the Ethernet/Cellular paths.

OFF: The Communicator module firmware can not be remotely upgraded. Local firmware upgrade is still possible.

[7] Alternate Test Transmissions

Default (OFF).

ON: When the periodic test transmission interval occurs, the test transmission will alternate between being sent to the primary and secondary receivers with each test transmission interval.

OFF: When the periodic test transmission interval occurs, the test transmission will be sent to the programmed receivers, based on the settings of the periodic test transmission reporting codes.

[8] Cellular Low Signal Trouble.

Default (OFF)

This option masks the Low Signal trouble from generating Cellular trouble.

ON: A Cellular Trouble event is generated when the radio signal level falls below threshold level (average CSQ level is 4 or less).

OFF: A Cellular Trouble event is **not** generated when the radio signal level falls below threshold level (average CSQ level is 4 or less).

[006] System Toggle Options 2

[1] Ethernet 1 Receiver Enabled.
Default (ON) (OFF for 3G2060R).
ON: Ethernet Receiver 1 is enabled.
OFF: Ethernet Receiver 1 is disabled.

[2] Ethernet 2 Receiver Enabled.
Default (ON) (OFF for 3G2060R).
ON: Ethernet Receiver 2 is enabled.
OFF: Ethernet Receiver 2 is disabled.

[3] Reserved. ( ).

[4] Cellular 1 Receiver Enabled.
Default (ON).(OFF for TL2603GR)
ON: Cellular Receiver 1 is enabled.
OFF: Cellular Receiver 1 is disabled.

[5] Cellular 2 Receiver Enabled.
Default (ON).(OFF for TL2603GR)
ON: Cellular Receiver 2 is enabled.
OFF: Cellular Receiver 2 is disabled.

[6] Reserved ( ).

[7] DLS Over Cellular.
Default (ON).

NOTE: Program this toggle as OFF if you want to completely disable DLS from using the Cellular path.

ON: DLS is enabled on the Cellular path.
OFF: DLS is disabled on the Cellular path.

NOTE: If this Toggle is OFF, DLS sessions will occur on the Ethernet path only, regardless of Primary Path set in Section [005] Toggle Option [4]. If it is ON then the Communicator will connect to the Primary path first for DLS and if the session fails, the Secondary path will be used.

[8] Reserved ( ).

[007] DNS Server IP 1

Default (000.000.000.000)

*Programming this Section is **not** permitted on a UL/ULC listed system.*

Enter the IP address for DNS Server 1. Format is 4 fields, each field is a 3 digit decimal. Valid range: 000-255.

NOTE: If no value is programmed and DHCP is used, the DHCP Server will configure the address. If an address is programmed and DHCP is used, the address that you program will be used instead of the DHCP address.

[008] DNS Server IP 2

*Programming this Section is **not** permitted on a UL/ULC listed system.*

Default (000.000.000.000)

Enter the IP address for DNS Server 2. Format is 4 fields, each field is a 3 digit decimal. Valid range: 000-255.

NOTE: If no value is programmed and DHCP is used, the DHCP Server will assign this value. If an address is programmed and DHCP is used, the address that you program will be used instead of the DHCP address.

Programming Options

[011] Installer Code

Default (CAFE)

Program your installer code for this Communicator module. The installer code will be required when programming the Communicator module. Valid range: 0000 - FFFF.

[012] DLS Incoming Port

Default (0BF6/3062)

The DLS Incoming Local Port (listening port) is the port DLS IV will use when connecting to the Communicator. If a router or gateway is used, it must be programmed with a Transmission Control Protocol (TCP) port forward for this port to the Communicator module IP address. Valid range: 0000 - FFFF.

[013] DLS Outgoing Port

Default (0BFA/3066)

The DLS Outgoing Port is used for outgoing session to DLS IV after an SMS request has been sent to the Communicator. Use this Section to set the value of the local outgoing port. The value must be changed 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 range: 0000-FFFF.

NOTE: If Section [006] Toggle Option [7] is ON, DLS will use the Primary path for session. If Section [006] Toggle Option [7] is OFF DLS will use the Ethernet path, if available.

[021] Account Code

Default (FFFFFF)

The account code is included when transmitting any events generated by the Communicator. (e.g., Panel Absent Trouble). It is recommended that the account code be the same as the control panel account number. Valid range: 00000**1**-FFFFF**E**. If 4 digit account codes are needed the 2 lowest digits shall be programmed as FF (e.g., Account 1234 is programmed as:1234**FF**).

NOTE: Programming this Section with all 0 or F will cause a Module Configuration Trouble.

NOTE: This section shall sync with Panel Option [310] with Panel version 4.50 or higher.

[022] Communications Format

Default (04)

Program 03 for Contact ID (CID). Program 04 for SIA. The module can be configured to send Events in SIA or CID format. The SIA communication format follows the level 2 specifications of the *SIA Digital Communication Standard - October 1997*. This format will send the account code along with its data transmission. The transmission will look similar to the following at the receiver.

NOTE: This section shall sync with panels version 4.50 or higher.

Example:

Nri0 ET001 where: **N** = New Event; **ri0** = Partition/Area identifier; **ET** = Panel Absent Trouble; **001** = Zone 001.

Communications Reporting Codes

Table 7: Communications Reporting Codes

Event	SIA Identifier	SIA Reporting Code	CID Qualifier	CID Event Code	CID Reporting Code	CID User/ Zone
[023] Panel Absent Trouble	ET	001	1	3	55	001
[024] Panel Absent Trouble Restore	ER	001	3	3	55	001
[025] Radio Activation Restore	RS	001	3	5	52	001
[026] Ethernet 1 Test Transmission	RP	001	1	6	A3	951
[027] Ethernet 2 Test Transmission	RP	002	1	6	A3	952
[028] Cellular 1 Test Transmission	RP	003	1	6	A3	955
[029] Cellular 2 Test Transmission	RP	004	1	6	A3	956
[030] FTC Restore	YK	001	3	3	54	001

[023] Panel Absent Trouble

Default (FF)

Program 00 to disable this event or FF to enable. This event will occur when communications with the panel have been lost for more than 60 seconds.

[024] Panel Absent Trouble Restore

Default (FF)

Program 00 to disable this event or FF to enable. This event will occur when communications with the control panel have resumed.

[025] Radio Activation Restore

Default (FF)

Program 00 to disable this event or FF to enable. This event will occur after any successful Connect24 programming session.

System Test Options [026 - 029]

Test Transmissions to Primary Receiver, with Backup to Secondary Receiver:

Set Ethernet Section [026] to (FF); [027] to (00). Set Cellular Section [028] to (FF); [029] to (00).

- If the test transmission fails to the primary receiver it will backup to the secondary receiver.
- If the test transmission fails to the secondary receiver an FTC trouble will be generated.

Test Transmission Unique to Primary and Secondary Receivers:

Set Ethernet Section [026] to (FF); [027] to (FF). Set Cellular Section [028] to (FF); [029] to (FF).

- The module will send periodic test transmissions to each receiver independently, with no backups.
- If the test transmission fails to any of the programmed receivers, an FTC trouble will be generated.

Alternate Test Transmission:

Alternate Test Transmission can be enabled or disabled in Section [005] Toggle Option [7].

Alternate Test Transmission with backup receivers:

Set Ethernet Section [026] to (FF); [027] to (00). Set Cellular Section [028] to (FF); [029] to (00).

Interval 1:

- If the test transmission fails to the primary receiver it will backup to the secondary receiver.
- If the test transmission fails to the secondary receiver an FTC trouble will be generated.

Interval 2:

- If the test transmission fails to the secondary receiver it will backup to the primary receiver.
- If the test transmission fails to the primary receiver an FTC trouble will be generated.

Test Transmission Unique to Primary and Secondary Receivers:

Set Ethernet Section [026] to (FF); [027] to (FF). Set Cellular Section [028] to (FF); [029] to (FF).

Interval 1:

- The module will send periodic test transmissions to Primary receivers (Ethernet Primary and Cellular Primary) independently, with no backups.
- If the test transmission fails to any of the programmed primary receivers, an FTC trouble will be generated

Interval 2:

The module will send periodic test transmissions to Secondary receivers (Ethernet Secondary and Cellular Secondary) independently, with no backups.

- If the test transmission fails to any of the programmed secondary receivers, an FTC trouble will be generated

[026] Ethernet 1 Transmission

Default (FF)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

[027] Ethernet 2 Transmission

Default (00)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

[028] Cellular 1 Transmission

Default (FF)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

[029] Cellular 2 Transmission

Default (00)

Program 00 to disable this event transmission or FF to enable. See System Test Options (above) for details on settings.

NOTE: The time interval (in minutes) between periodic tests is programmed in Section [125] (Ethernet) and Section [225] (Cellular).

[030] FTC Restore

Default (FF)

Program 00 to disable this event transmission or FF to enable. This event will occur when an FTC Trouble on the system restores.

[033] Communicator Firmware Update Begin

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the communicator firmware update begins.

[034] Communicator Firmware Update Successful

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the communicator firmware update successfully completed.

[035] Panel Firmware Update Begin

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware update begins.

[036] Panel Firmware Update Successful

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware is updated successfully.

[037] Panel Firmware Update Fail

Default (FF);

Program 00 to disable this event transmission or FF to enable. This event will occur when the panel firmware updated has failed.

Table 8: Panel Tamper Alarm Restore

Event	SIA Identifier	SIA Reporting Code	Contact ID Qualifier	Contact ID Event Code	Contact ID Reporting Code	Contact ID User/Zone
[033] Comm. FW Update Begin	LB	00	1	9	03	002
[034] Comm. FW Update Successful	LS	00	3	9	03	002
[035] Panel FW Update Begin	LB	00	1	9	03	003
[036] Panel FW Update Successful	LS	00	3	9	03	003
[037] Panel FW Update Fail	LU	00	1	9	04	003

Ethernet Receiver 1 Options

[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 to the central station receiver. Signals received from the Panel will use the control panel account number. Valid range: 000000000**1**-FFFFFFFFF**E**. Programming all **0** or all **F** will cause a Module Configuration Trouble.

NOTE: If Ethernet Receiver 1 and Cellular Receiver 1 are programmed as the same receiver (IP and port number are identical), Ethernet Receiver 1 account code will be used.

[102] Ethernet Receiver 1 DNIS

Default (000000)

The dialed Number Information Service (DNIS) is used in addition to the Account Code to identify the Communicator module at the central station. Valid range: 000000 - **0**99999. Value is entered as a leading 0 followed by the 5 digit DNIS. Format is Binary Coded Decimal (BCD).

NOTE: Each Ethernet/Cellular receiver must be programmed with a unique DNIS.

[103] Ethernet Receiver 1 Address

Default (127.000.000.001)

The default address 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. Typically used 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.

NOTE: When a valid IP address has been programmed, Ethernet Receiver 1 is enabled and will communicate events over the Ethernet channel.

Ethernet Receiver 1 and Cellular Receiver 1 may be configured to communicate to the same central station receiver. To configure the device to operate using this Common Receiver Mode functionality, program Ethernet Receiver 1 and Cellular Receiver 1, IP address and port number with identical values.

NOTE: When operating in Common Receiver Mode, Ethernet Receiver 1 account code will be used for Ethernet and Cellular.

[104] Ethernet Receiver 1 Remote Port

Default (0BF5/3061)

This Section determines the remote port of Ethernet receiver 1. Valid range: 0000 - FFFF.

[105] Ethernet Receiver 1 Local Port

Default (0BF4/3060)

Use this Section to set the value of the local outgoing port. Set the value of this port when your installation is located behind a firewall and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

[106] Ethernet Receiver 1 Domain Name

Default ( )

Enter the Domain Name as 32 ASCII characters.

*Programming this section is **not** permitted on a UL/ULC listed system.*

Ethernet Receiver 2 Options

[111] Ethernet Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between transmitters. The 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 range: 000000000**1**-FFFFFFFFF**E**. Programming all **0** or all **F** will cause a Module Configuration Trouble (yellow LED=12 flashes).

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

[112] Ethernet Receiver 2 DNIS

Default (000000)

The DNIS is used in addition to the account code to identify the Communicator module at the central station. Valid range: 000000 - **0**99999. Value is entered as leading **0** followed by the 5-digit DNIS. Format is BCD.

NOTE: Each Ethernet/Cellular receiver must be programmed with a unique DNIS.

[113] Ethernet Receiver 2 Address

Default (000.000.000.000)

Programming the Ethernet Receiver 2 IP address with 000.000.000.000 will disable Ethernet.

Enter the Ethernet receiver 2 IP address. This address will be provided by your central station system administrator. Format is 4 fields, each field is a 3-digit decimal. Valid range: 000-255.

NOTE: When a valid IP address has been programmed, Ethernet Receiver 2 is enabled and will communicate events over the Ethernet channel.

Ethernet Receiver 2 and Cellular Receiver 2 may be configured to communicate to the same central station receiver.

To configure the device to operate using this common receiver mode functionality, program the Ethernet Receiver 2 and Cellular Receiver 2, IP address and port number with the same values. When operating in common receiver mode the Ethernet Receiver 2 account code will be used for communications over Ethernet and Cellular.

NOTE: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 to communicate to same receiver.

[114] Ethernet Receiver 2 Remote Port

Default (0BF5/3061)

This Section is used to program the port number used by Ethernet Receiver 2. Set the value of this port when your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

NOTE: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 Port with the same value.

[115] Ethernet Receiver 2 Local Port

Default (0BF9/3065)

Use this Section to program the value of the local outgoing port. You can set the value of this port when your installation is located behind a firewall and must be assigned a particular port number as determined by your network administrator. Valid range: 0000 - FFFF.

NOTE: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 Port with the same value.

[116] Ethernet Receiver 2 Domain Name

Default ( )

*Programming this section is **not** permitted on a UL/ULC listed system.*

Enter the Domain Name as 32 Character ASCII.

Ethernet Options

[124] Ethernet Test Transmission Time

Default (9999)

Enter a 4 digit number (0000-2359) using the 24-hour clock format (HHMM) to set the test transmission time of day. Valid range: 00 - 23 hours (HH) and 00 - 59 minutes (MM). Programming a value of 9999 will disable the test transmission time.

NOTE: The internal date and time will automatically be programmed when the unit communicates with the primary receiver.

[125] Ethernet Test Transmission Cycle

Default (000000)

This value represents the interval between test transmissions, in minutes. Valid range: 000000 - 999999 minutes. Once the unit has sent the initial periodic test transmission, all future test transmissions will be offset by the programmed number of minutes. See Sections [026] - [029].

Table 9: Ethernet Test Transmission Interval

Test Transmission Interval	Daily	Weekly	Monthly
Programmed Minutes	001440	010080	043200

NOTE: Minimum value is 000005 minutes. Programming an interval that is less than 5 minutes will disable test transmission.

Cellular Receiver 1 Options

[201] Cellular 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 range: 000000000**1** - FFFFFFFFF**E**. Programming all **0** or all **F** will cause a Module Configuration Trouble (yellow LED = 12 flashes).

[202] Cellular Receiver 1 DNIS

Default (000000)

The DNIS is used in addition to the account code to identify the Communicator module at the central station. Valid range: 000000 - **0**99999. Values are entered as leading **0** followed by the five digit DNIS. Format is BCD.

NOTE: Each Ethernet/Cellular receiver must be programmed with a unique DNIS.

[203] Cellular Receiver 1 Address

Default (000.000.000.000)

Enter the Cellular Receiver 1 IP address. This information will be provided by your central station system administrator. Each 3-digit segment of the address must be within a valid range of 000-255.

NOTE: When a valid IP address has been entered, the Cellular is enabled and will communicate events over the Cellular channel.

[204] Cellular Receiver 1 Port

Default (0BF5/3061)

This Section determines the port used by Cellular Receiver 1. Change the default value of this port when your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

NOTE: Programming this section with 0000 will disable the receiver.

[205] Cellular Receiver 1 APN

Default ( )

The Access Point Name (APN) determines the Cellular network that the Communicator will connect to. This information is available from your network carrier. Program this Section as 32 ASCII characters.

NOTE: When a SIM card with a custom APN is used, the unit will not have access to the Internet. DLS and remote flash can still be done if Section [221] is programmed with a valid Public APN.

[206] Cellular Receiver 1 Domain Name

Default ( )

*Programming this section is **not** permitted on a UL/ULC listed system.*

Enter the Domain Name as 32 ASCII characters. This information will be provided by your central station system administrator.

Cellular Receiver 2 Options

[211] Cellular Receiver 2 Account Code

Default (0000000000)

The account code is used by the central station to distinguish between different transmitters. This account code is used when transmitting signals to the central station receiver. Signals received on the panel will use the panel account number. Valid range: 000000000**1** - FFFFFFFFF**E**.

NOTE: Programming this Section as all 0 or F will cause a Module Configuration Trouble (yellow LED = 12 flashes).

[212] Cellular Receiver 2 DNIS

Default (000000)

The DNIS is used in addition to the Account Code to identify the Communicator module at the central station. Valid range: 000000 - **0**99999. Values are entered as a 0 followed by the 5 digit DNIS value. Format is BCD.

NOTE: Each Ethernet/Cellular receiver must be programmed with a unique DNIS.

[213] Cellular Receiver 2 Address

Default (000.000.000.000)

Enter the Cellular Receiver 2 IP address. This IP address will be provided by your central station. Format is 4 fields, each field is 3-digit decimal. Valid range: 000 - 255.

NOTE: When a valid address has been entered, Cellular Receiver 2 is enabled and will communicate events over the Cellular path.

[214] Cellular Receiver 2 Port

Default (0BF5/3061)

This Section defines the port of Cellular Receiver 2. Change the value of this port when your installation is located behind a firewall and must be assigned a particular port number, as determined by your central station system administrator. Valid range: 0000 - FFFF.

NOTE: Do not program Cellular Receiver 1 and Cellular Receiver 2 to communicate to the same receiver.

[215] Cellular Receiver 2 APN

Default ( )

The APN determines the Cellular network that the Communicator will connect to. This information is available from your network carrier. Program this Section with up to 32 ASCII characters.

NOTE: When a SIM card with a custom APN is used, the unit will not have access to the internet. DLS and remote flash can still be done if Section [221] is programmed with a valid Public APN.

[216] Cellular Receiver 2 Domain Name

Default ( )

*Programming this section is **not** permitted on a UL/ULC listed system.*

Enter the Cellular Receiver 2 Domain Name with up to 32 ASCII characters.

Cellular Options

[221] Cellular Public Access Point Name

Default ( )

When the Communicator is operating on a private APN, use this Section to select a public APN for DLS and Remote Firmware Update. This information is available from your network carrier. The APN identifies the public Cellular network that the Communicator will connect to.

[222] Cellular Login User Name

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Program your login User Name in this Section. Format is up to 32 ASCII characters.

[223] Cellular Login Password

Default ( )

Some network carriers require you to provide login credentials when connecting to an APN. Program your login Password in this Section. Format is up to 32 ASCII characters.

[224] Cellular Test Transmission Time of Day

Default (9999)

Enter a 4 digit value using the 24-hour clock format (HHMM) to set the test transmission time of day. Valid range: 00-23 for the hours (HH) and 00-59 for the minutes (MM).

NOTE: To disable the test transmission time of day enter 9999 or FFFF in this Section.

The internal date and time will be automatically programmed by the primary receiver only.

[225] Cellular Test Transmission Cycle

Default (000000)

This value represents the interval in between test transmissions in minutes. Valid range: 000000 - 999999 minutes. Once the unit has sent the initial periodic test transmission, all future test transmissions will be offset by the programmed number of minutes. See Sections [026] - [029].

Table 10: Cellular Test Transmission Interval

Test Transmission Interval	Daily	Weekly	Monthly
Programmed Minutes	001440	010080	043200

NOTE: Minimum value is 000005 minutes. Programming an interval that is less than 5 minutes will disable test transmission.

[226] Cellular Trouble Delay

Default (0A)

This option is used to program the delay, in minutes, for reporting a Cellular Trouble Delay. Valid entries are 00 - FF. (e.g., for a 10 minute Cellular Trouble Delay enter: **0A**). There is no reporting delay if value is programmed as 00.

Receiver Diagnostic Testing

[901] Diagnostic Test Transmission

[1]Ethernet 1 (OFF).
[2] Ethernet 2 (OFF).
[3] Cellular 1 (OFF).
[4] Cellular 2 (OFF).
[5],[6],[7],[8] Reserved(OFF).
This Section may be used by the installer to force the Communicator to send an immediate test transmission to specific receivers, to verify that the communications paths are available. Diagnostic Test Transmission failure will indicate as FTC trouble (Yellow LED = 9 flashes). If an FTC error occurs when testing all receivers, select only one receiver and repeat test to isolate the receiver that is not communicating.

NOTE: Sending a test transmission to a receiver that is not programmed generates FTC trouble.

System Information (Read Only)

NOTE: Sections [987] - [998] are provided for information (Read Only). Values in these sections cannot be modified by the Installer.

[987] Language Version

This section will display the current Language version of the Communicator.

[988] DNS 1 IP Address

This section will display the IP address of DNS Server 1. This is useful when the unit is configured for DHCP and you need to see the IP address was assigned to the device by the DHCP Server. This value is programmed in Section [007] or assigned by DHCP.

[989] DNS 2 IP Address

This section will display the IP address of DNS Server 2. This is useful when the unit is configured for DHCP and you need to see the IP address that was assigned to the device by the DHCP Server. This value is programmed in Section [008] or assigned by DHCP.

[990] Boot Loader Version

This section will display the current Boot Loader version of the Communicator.

[991] Firmware Version

This section will display the current firmware version of the device. Update worksheets with new version after a flash update is completed.

[992] Ethernet IP Address

This section will display the IP address of the Ethernet connection. This value is programmed in Section [001] or assigned by DHCP.

[993] Ethernet Gateway Address

This section will display the IP address of the Ethernet Gateway. This value is programmed in Section [003] or assigned by DHCP.

[994] Cellular IP Address

This section will display the current dynamic IP address assigned by DHCP to the Cellular connection.

NOTE: Cellular uses DHCP (Dynamic IP) only. The Cellular IP address is always provided by the Cellular network (i.e., not programmable).

[995] SIM Number

This section will display the Subscriber Identity Module (SIM) number of the SIM card installed in the Communicator. Format is: Major Industry Identifier (2 digits) Mobile Country Code (2 or 3 digits); Mobile Network Code (2 - 3 digits); Unique Number (10 - 12 digits); and Checksum (1 digit). Valid SIM numbers range is: 18 - 21 numbers. This number is printed on SIM and the outside of the Communicator carton.

NOTE: The Checksum digit is omitted on 19-digit SIM Card numbers.

[996] Cellular Telephone Number

NOTE: This section will display the Cellular telephone number of the SIM. This telephone number is required by the Installer for DLS and remote firmware (flash) update. User can access this telephone number by entering [*] [6] < > "Cellular Phone No." to display the phone number.

[997] IMEI Number

This section will display the unique 15-digit International Mobile Equipment Identity (IMEI) of the radio. Format is: Reporting Body Identifier (2 digits), Allocation Number (4 digits); Final Assembly Code (2 digits); Serial Number (6 digits); and a check digit.

[998] MAC Address

This section will display the unique12-digit, hexadecimal number assigned as the Media Access Control (MAC) address of the device.

System Reset Defaults

[999] Software Default

Default (99);

The Software default allows the installer to refresh the unit after changes and also return the Communicator to the default state.

00: **Default Module**. All programming Sections in module revert to factory settings. This will erase all existing programming of the unit.

55: Reset. The Communicator is reset. This option is equivalent to power cycling the Communicator.

Communicator Status, Initialization, Diagnostics and Troubleshooting

[983] Firmware Update Diagnostics Section

NOTE: This section is not real-time, you will have to exit and return to the section to see if the status has been changed

Firmware updates for panel and the communicator itself can be made from the communicator.

- The Firmware Update Diagnostic section is a Read Only 2 Digit, Hexadecimal Section
- File download has begun, Section [983] is updated with 0xFD reason code
- The default value of this location is 0xFE, indicating no errors
- Though the Communicator can reject Firmware Download SMS String for several reasons. it will be shown with 0xFF reason code for Firmware Receive Failure. This failure can occur if:
  - A DLS Session is in progress
  - C24 Programming is in Progress
  - Remote firmware upgrade is disabled
  - TFTP Firmware Update Download is in progress
  - iControl/iHub Firmware Update is in progress
  - the download got dropped/cancelled, section [983] will get updated with 0xFF reason code
- Upon successful download, the communicator will either be updating itself, or the panel
- After a Communicator Firmware Upgrade, the communicator enters a 4.5-minute window before performing the update. This allows it to communicate with the Central Station and interactive services . Section [983] will get updated with a 0x0A reason code, indicating communication is in progress.
- During Panel Firmware Update, if panel firmware pushes through, the user will be able to see it because the keypad enters keybus fault. If panel rejects firmware for any reason, the communicator shall update section [983] with the cancellation reason code provided by the panel
- In the Case of Communicator Firmware Update successful, the communicator shall update diagnostic section to 0xFB after it is updated successfully
- During Panel Firmware Update Sequence, the Panel could Cancel the Firmware Update due to the Reasons Codes shown in Table 17.
- Upon Success of Panel Firmware Upgrade, section [983] will get updated with 0xFC to indicate Panel Firmware Update Complete.
- Reason codes and corresponding firmware images are displayed in the table below.

NOTE: Firmware Update Status shows one update process at a time. If communicator and panel updates take place simultaneously, panel related status takes priority.

Table 11: Reason Codes Description and Corresponding Firmware Images

Reason Code	Description of Reason Code	Firmware Image is
00	Version Check Failed	Image Erased
01	Image Type Mismatch	Image Erased
02	Panel Type Mismatch	Image Erased
03	Hardware Type Mismatch	Image Erased
04	Firmware header Wrong Length	Image Erased
05	Panel is Armed	Firmware Update Pending Status Clearance
06	AC Trouble	Firmware Update Pending Status Clearance
07	Low Battery	Firmware Update Pending Status Clearance
08	Unviewed Alarm	Firmware Update Pending Status Clearance
09	FTC Trouble	Firmware Update Pending Status Clearance
0A	Communication in Progress	Firmware Update Pending Status Clearance
0B	Software Variant Mismatch	Image Erased
FB	Communicator Firmware Update Complete	n/a
FC	Panel Firmware Update Complete	n/a
FD	File Download in Progress	n/a
FE	Firmware File Empty	Software Default Value (Factory Default)
FF	File Receive Failure	File Was Not Received
F1	Communicator Update Fail	Firmware Update did Not Occur
F2	Panel Update Fail	Panel is not responding

The table above displays the firmware update indicator codes and meaning of each code. The updates can be made from communicator. Communicator can update firmware of the panel and also of communicator itself. This section does not provide specific details such as if the Image is still stored or erased due to the cancellation code. Specific details shall be captured in User/Installation Manuals and provided to Technical Advice Bulletin.

For the Purpose of Documentation:

- Communicator shall erase panel image file on Reason Code 0x00 ~ 0x04 and 0x0B
- Communicator shall try to upgrade panel image file forever on Reason Code 0x05 ~ 0x0A.

[984] Communicator Status

NOTE: This section is not real-time, you will have to exit and return to the section to see if the status has been changed

The communicator status sections provide the installer with the status of the communicator's functionality, operational readiness, and failures.

The communicator status is displayed as a 6-digit hexadecimal code. The code ranges between 00000F and 2220CF, though not all numbers in this range are assigned. Each of the 6 digits represents a status or trouble indicator as below:

1. Digits 1 & 2: Signal strength indicators display the presence/strength of cellular radio.
2. Digit 3: Network Indicator, indicates the operational status of the network.
3. Digits 4 & 5: Trouble Indicator displays the type of issue on the communicator or modules associated with and connected to communicator.
4. Digit 6: Reserved, displayed a an 'F' or a '-', for example '11002-'.

To understand the communicator status better, consider status code 11002F as an example:

11- Signal strength is excellent

0 - No network issues

02 - Panel Supervision trouble with the communicator

Communicator Troubleshooting

The status code for the radio signal strength, its typical troubles, possible causes and troubleshooting instructions is displayed in the table below.

Table 12: Radio Signal Strength - Digits 1 and 2

Signal Strength	CSQ Level	Signal Indicator 1	Signal Indicator 2	Signal Level [dBm]	Signal Level Status	Action Required
No Signal	0	0	0	-108.8	bad	Check all antenna connections. Confirm cellular service is active in area. Relocate Panel or install external antenna.
1 Bar	1 - 4	0	2	-108 ~ -103	weak	Relocate Panel or install external antenna if Yellow Trouble LED has: 5 flashes.
2 Bars	5 - 6	0	1	-102 ~ -99	weak	
3 Bars	7 - 10	2	1	-98 ~ -91	strong	**Location is OK.** Cellular Signal Strength is greater than CSQ 7.
4 Bars	11 - 13	2	1	-90 ~ -85	strong	
5 Bars	14 +	1	1	-84 and higher	excellent	

Table 13: Network Indicator - Digit 3

Network indicator Value	Means
OFF	No Network Trouble
ON	Ethernet Cable disconnected Ethernet DHCP failed Radio connection has been rest Radio IP failed
Flashing	Incoming transmission Connect 24 programming Outgoing transmission Incoming transmission

Table 14: Trouble Code Indications - Digits 4 & 5

Trouble Indicator Digit	Trouble Type	Trouble Causes
00	No Trouble	N/A
02	Panel Supervision Trouble	Check Section [382]Toggle Option[5] is ON (Cellular/Ethernet Module Enabled). Ensure the PC-LINK cable between the Panel and Communicator is connected properly (not reversed) and is securely in place.
04	Lockout Trouble	The SIM card has incorrect PIN programmed or has a PIN that the module does not recognize. Replace the SIM card.
05	3G/Cellular Trouble	Confirm that cellular service is available and active in your area. Check all antenna connections. Ensure average radio signal strength is CSQ 5 or higher. Ensure the SIM card is properly inserted into the SIM card holder. Ensure the SIM card has been activated. (Could take up to 24 hrs after install). If this trouble persists, relocate the Panel (and Communicator) or install an external antenna extension kit.
06	Ethernet Trouble	Check with your ISP to confirm Internet service is active in your area. Ensure your Ethernet cable is securely inserted into the RJ45 jack of the Communicator and the Hub/Router/ Switch. Check that the link light on the Hub/Router/ Switch is ON. If link light is OFF, try restarting the Hub/Router/ Switch. If DHCP is used, ensure that the unit has an assigned IP address from the server. In Section [851] [992] verify a valid IP address is programmed. If not, contact the Network administrator. If problem persists, replace the Ethernet cable and RJ45 connector.
07	Receiver Not Available	Ensure that the Ethernet path has internet connectivity. If you are using a static IP address make sure the gateway and subnet mask are entered correctly. 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 for DHCP or have the proper IP address and port number. Ensure the cellular Receiver APNs have been programmed with the Access Point Name provided by your cellular provider.

Trouble Indicator Digit	Trouble Type	Trouble Causes
08	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.
09	FTC Trouble	The unit has exhausted all communications attempts to all programmed receivers for events generated by the Communicator. Restart the system. If trouble persists, contact your dealer.
0A	Connect24 Configuration Failure	The SIM is active but there is no programming for the Communicator. Ensure a profile has been programmed in Connect-24 for the SIM. You can confirm your programming by calling the Connect-24 VRU, or by logging into the Connect24 VRU web site.
0C	Module Configuration Trouble	This indication appears when Section [021] System Account Code, Section [101], [111], [201], and [211] Receiver Account Code have not been programmed. Ensure that a valid account code has been entered in these Sections.

[985] Radio Initialization Status

NOTE: This section is not real-time, you will have to exit and return to the section to see if the status has been changed

The radio initialization status provides installers with the status of radio communication. It is displayed as an 8-digit toggle option, with each digit indicating a task in the initialization process of

1. Radio power up
2. Received the SMS from C24
3. Radio reset
4. Radio attached to network
5. Receiver 1 Initialized
6. Receiver 2 Initialized
7. Receiver 3 Initialized
8. Receiver 4 Initialized

For example, the radio initialization status code 12-45--- indicates that Radio has been powered up, it has received SMS signal from C24, the radio is attached to the network, and Receiver 1 has been initialized. This code could be followed with...567 if Receivers 2, 3, and 4 are initialized where applicable.

If the radio initialization status code does not indicate any problems, proceed with installation as per this manual. If troubles are reported, reset the initialization process. If this action does not fix the problem, refer to Trouble shooting section in this manual.

The following table shows each digit position in the status code, each digit's value and its assigned meaning in the eight-digit code:

Table 15: Radio Initialization Status - 1-8 bits completion

Bit	1	2	3	4	5	6	7	8
Not Completed	-	-	-	-	-	-	-	-
Completed	1	2	3	4	5	6	7	8

ETHERNET/CELLULAR PROGRAMMING WORKSHEETS

System Options

[001] Ethernet IP Address

Default (000.000.000.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

[002] Ethernet IP Subnet Mask

Default (255.255.255.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

[003] Ethernet Gateway IP Address

Default (000.000.000.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

[004] Receiver Supervision Interval

Default (0087/135) Valid range: 0000 - FFFF.

|___|___|___|___|

[005] System Toggle Options

|___| [1] Ethernet Receiver 1 Supervised Default (OFF).
|___| [2] Cellular Receiver 1 Supervised Default (OFF).
|___| [3] Supervision Type Default (OFF).
|___| [4] Primary Communications Path.

[ON] 3G2060R.

|___| [5] Redundant Communications Default (OFF).
|___| [6] Remote Firmware Upgrade Default (ON).
|___| [7] Alternate Test Transmission Default (OFF).
|___| [8] Cellular Low Signal Trouble Default (OFF).

[006] System Toggle Options 2

|___| [1] Ethernet Receiver 1 Enabled Default (ON).
|___| [2] Ethernet Receiver 2 Enabled Default (ON).
|___| [4] Cellular Receiver 1 Enabled Default (ON).
|___| [5] Cellular Receiver 2 Enabled Default (ON).
|___| [7] DLS Over Cellular Default (ON).
|___| [8] Interactive Over Cellular Default (ON).

[007] DNS Server IP 1

Programming not permitted on UL/ULC listed system.

Default (000.000.000.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

[008] DNS Server IP 2

Programming not permitted on UL/ULC listed system.

Default (000.000.000.000)

|___|___|___|___|___|___|___|___|___|___|___|___|

Programming Options

[011] Installer Code

Default (CAFE) Valid range: 0000 - FFFF.

|___|___|___|___|

[012] DLS Incoming Port

Default (0BF6/3062) Valid range: 0000 - FFFF.

|___|___|___|___|

[013] DLS Outgoing Port

Default (0BFA/3066) Valid range: 0000 - FFFF.

|___|___|___|___|

[022] Communications Format

Default (04) Program 03 (CID), 04 (SIA).

|___|___|

[023] Panel Absent Trouble

Default (FF); Program 00 disable or FF enable.

|___|___|

[024] Panel Absent Trouble Restore

Default (FF) Program 00 disable or FF enable.

|___|___|

[025] Radio Activation Restore

Default (FF) Program 00 disable or FF enable.

|___|___|

System Test Options [026 - 029]

[026] Ethernet 1 Transmission

Default (FF) Program 00 disable or FF enable.

|___|___|

[027] Ethernet 2 Transmission

Default (00) Program 00 disable or FF enable.

|___|___|

[028] Cellular 1 Transmission

Default (FF) Program 00 disable or FF enable.

|___|___|

[029] Cellular 2 Transmission

Default (00) Program 00 disable or FF enable.

|___|___|

[030] FTC Restore

Default (FF) Program 00 disable or FF enable.

|___|___|

[033] Communicator Firmware Update Begin

Default (FF) Program 00 disable or FF enable.

|___|___|

[034] Communicator Firmware Update Successful

Default (FF) Program 00 disable or FF enable.

|___|___|

[035] Panel Firmware Update Begin
Default (FF) Program 00 disable or FF enable.
|__|__|

[036] Panel Firmware Update Successful
Default (FF) Program 00 disable or FF enable.
|__|__|

[037] Panel Firmware Update Fail
Default (FF) Program 00 disable or FF enable.
|__|__|

Ethernet Receiver 1 Options

[101] Ethernet Receiver 1 Account Code
Default (0000000000)
Valid range: 0000000001 - FFFFFFFFFE.
|__|__|__|__|__|__|__|__|__|__|

[102] Ethernet Receiver 1 DNIS
Default (000000) Valid range: 000000 - FFFFFF.
|__|__|__|__|__|__|

[103] Ethernet Receiver 1 Address
Default (127.000.000.001)
|__|__|__|__|__|__|__|__|__|__|__|__|

[104] Ethernet Receiver 1 Remote Port
Default (0BF5/3061) Valid range: 0000 - FFFF.
|__|__|__|__|

[105] Ethernet Receiver 1 Local Port
Default (0BF4/3060)Valid range: 0000 - FFFF.
|__|__|__|__|

[106] Ethernet Receiver 1 Domain Name
Default ( ) 32 ASCII characters.
Programming not permitted on UL/ULC listed system.

Ethernet Receiver 2 Options

[111] Ethernet Receiver 2 Account Code
Default (0000000000)
Valid range: 0000000001 - FFFFFFFFFE.
|__|__|__|__|__|__|__|__|__|__|

[112] Ethernet Receiver 2 DNIS
Default (000000) Valid range: 000000 - 0FFFFF.
|__|__|__|__|__|__|

[113] Ethernet Receiver 2 Address
Default (000.000.000.000)
|__|__|__|__|__|__|__|__|__|__|__|__|

[114] Ethernet Receiver 2 Remote Port
Default (0BF5/3061) Valid range: 0000 - FFFF.
|__|__|__|__|

[115] Ethernet Receiver 2 Local Port
Default (0BF9/3065) Valid range: 0000 -FFFF.
|__|__|__|__|

[116] Ethernet Receiver 2 Domain Name Default ( )
Programming not permitted on UL/ULC listed system.

Ethernet Options

[124] Ethernet Test Transmission Time
Default (9999) Valid: 00-23(HH); 00-59(MM)
|__|__|__|__|

[125] Ethernet Test Transmission Cycle
Default (000000)
Valid range: 000000 - 999999 minutes.
|__|__|__|__|__|__|

Cellular Receiver 1 Options

[201] Cellular Receiver 1 Account Code
Default (0000000000)
Valid range: 0000000001 - FFFFFFFFFE.
|__|__|__|__|__|__|__|__|__|__|

[202] Cellular Receiver 1 DNIS
Default (000000) Valid range: 000000 - 0FFFFF.
|__|__|__|__|__|__|

[203] Cellular Receiver 1 Address
Default (000.000.000.000). Valid range: 000-255.
|__|__|__|__|__|__|__|__|__|__|__|__|

[204] Cellular Receiver 1 Port
Default (0BF5/3061) Valid range: 0000 - FFFF.
|__|__|__|__|

[205] Cellular Receiver 1 APN Default ( )
32 ASCII characters.

---

[206] Cellular Receiver 1 Domain Name Default ( )
Programming not permitted on UL/ULC listed system.
32 Character ASCII characters.

Cellular Receiver 2 Options

[211] Cellular Receiver 2 Account Code
Default (0000000000)
Valid range: 000000000**1** - FFFFFFFFF**E**.
|__|__|__|__|__|__|__|__|__|__|

[212] Cellular Receiver 2 DNIS
Default (000000)
Valid range: 000000 - 0FFFFF.
|__|__|__|__|__|__|

[213] Cellular Receiver 2 Address
Default (000.000.000.000)
Valid segment range: 000-255
|___|___|___||___|___|___||___|___|___|___|___|___|

[214] Cellular Receiver 2 Port
Default (0BF5/3061) Valid range: 0000 - FFFF.
|___|___|___|___|

[215] Cellular Receiver 2 APN
Default ( ) 32 ASCII characters.

_____

[216] Cellular Receiver 2 Domain Name
Default ( )
Programming not permitted on UL/ULC listed system.
32 ASCII characters.

_____

Cellular Options

[221] Cellular Public Access Point Name
Default ( ) 32 ASCII characters

_____

[222] Cellular Login User Name
Default ( ) 32 ASCII characters.

_____

[223] Cellular Login Password
Default ( ) 32 ASCII characters.

_____

[224] Cellular Test Transmission Time of Day
Default (9999) Valid range: 00 - 23 hrs. (HH) 00 - 59 min. (MM).
|___|___|___|___|

[225] Cellular Test Transmission Cycle
Default (000000)
Valid range: 000000 - 999999 minutes.
|___|___|___|___|___|___|

[226] Cellular Trouble Delay
Default (10)
Valid entries from, 00 to FF.
|___|___|

[901] Diagnostic Test Transmission
|___| [1] Ethernet 1 Default (OFF).
|___| [2] Ethernet 2 Default (OFF).
|___| [3] Cellular 1 Default (OFF).
|___| [4] Cellular 2 Default (OFF).

System Information (Read Only)

[988] DNS 1 IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|

[989] DNS 2 IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|

[991] Firmware Version
|___|___|___|___|___|___|___|___|

[992] Ethernet IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|

[993] Ethernet Gateway Address
|___|___|___||___|___|___||___|___|___|___|___|___|

[994] Cellular IP Address
|___|___|___||___|___|___||___|___|___|___|___|___|

[995] SIM Number

_____

[996] Cellular Telephone Number
This number is required for DLS, and Firmware upgrades.

_____

[997] IMEI Number

_____

[998] MAC Address
|__|__|__|__|__|__||__|__|__|__|__|__|

System Reset Defaults

[999] Software Default
Default (99); Valid entries are 00 or 55
|___|___|

End User Licence Agreement

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 (DSC),** a division of Tyco Safety Products Canada Ltd., 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 EULA 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, under the following terms:.

GRANT OF LICENSE This EULA grants You the following rights:

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

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.

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.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

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.

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.

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.

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.

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.

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.

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

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.

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

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

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

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.

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 with non DSC software or hardware products.

LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK -In any event, if any statute implies warranties or conditions not stated in this license agreement, 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 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.

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.

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 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.

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 (DSC) warrants the original purchaser that for a period of twelve (12) 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; or
- 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: freight cost to the repair centre; products which are not identified with DSC's product label and lot number or serial number; or 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. 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 Digital Security Controls 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-3G260R

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following tow 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.

Cet appareil est conforme avec Industrie Canada exempts de licence standard RSS (s). Le fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne peut pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interferences qui peuvent causer un mauvais fonctionnement de l'appareil.

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.

29008306R003

© 2012 Tyco International Ltd. and its Respective Companies. All Rights Reserved.
Toronto, Canada • **www.dsc.com**
Tech Support: 1-800-387-3630 (CA, US), 905-760-3000
Printed in Canada

From Tyco Security Products