

# 3G2055-NA

HSPA/3G WIRELESS ALARM COMMUNICATOR

# TL255-NA

ETHERNET/INTERNET ALARM COMMUNICATOR

# TL2553G-NA

ETHERNET/INTERNET AND HSPA/3G/2G DUAL-PATH ALARM COMMUNICATOR

29007850R001\_Shared\_Review\_updated\_by\_MM\_04

**DSC**

*A Tyco International Company*



**v3.0**

**Installation Manual**

---

**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

Warning: Installer Please Read Carefully . . . . .	3
<b>General Information . . . . .</b>	<b>4</b>
<b>Communicator Technical Specifications . . . . .</b>	<b>5</b>
Features . . . . .	5
UL/ULC Installation Requirements . . . . .	5
Ratings . . . . .	6
Hardware Compatibility . . . . .	6
Software Compatability . . . . .	6
<b>Communicator Pre Installation Configuration. . . . .</b>	<b>6</b>
Connect24™ Account and SIM card Activation . . . . .	6
Encryption. . . . .	7
<b>Communicator Configuration with SCW . . . . .</b>	<b>7</b>
Installing CAT 5 Cable (TL2553G/TL255 only) . . . . .	7
Communicator Reset . . . . .	8
Establishing a Communication Channel with the SCW Panel. . . . .	8
Label Programming for SMS Message . . . . .	9
<b>Programming Options Sections</b>	
<b>ETHERNET/Cellular Programming Options . . . . .</b>	<b>10</b>
System Options . . . . .	10
Programming Options. . . . .	12
Communications Reporting Codes. . . . .	13
Ethernet Receiver 1 Options . . . . .	14
Ethernet Receiver 2 Options . . . . .	14
Ethernet Options . . . . .	15
Cellular Receiver 1 Options . . . . .	15
Cellular Receiver 2 Options . . . . .	16
Cellular Options. . . . .	16
Interactive Options. . . . .	17
Receiver Diagnostic Testing . . . . .	18
System Information (Read Only) . . . . .	18
System Reset Defaults . . . . .	19
<b>Programming Worksheets Sections</b>	
<b>Ethernet/Cellular Programming Worksheets. . . . .</b>	<b>21</b>
System Options . . . . .	21
Programming Options. . . . .	21
Ethernet Receiver 1 Options . . . . .	21
Ethernet Receiver 2 Options . . . . .	21
Ethernet Options . . . . .	22
Cellular Receiver 1 Options . . . . .	22
Cellular Receiver 2 Options . . . . .	22
Cellular Options. . . . .	22
Interactive Options. . . . .	22
Receiver Diagnostic Testing . . . . .	23
System Information (Read Only) . . . . .	23
System Reset Defaults . . . . .	23
<b>End User Licence Agreement . . . . .</b>	<b>24</b>
<b>Limited Warranty . . . . .</b>	<b>25</b>

**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 INFORMATION

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

### KEYPAD DATA DISPLAY

- **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 DATA FROM KEYPAD

To enter data at the keypad, press the number key, from the table below, to select the character that you want. Pressing the number key repeatedly will scroll through the characters available for that key. Press the [\*] key and use [<] [>] keys to scroll to one of the following selections: (Press [\*] to select the Option.)

- **ASCII Entry.** Use this mode to enter ASCII characters from the keypad.
- **Clear to End.** This selection will clear the remainder of the display.
- **Clear Display.** This selection will completely erase all entries on the display.
- **Change Case.** Toggles between upper/lower depending on current selection.

**NOTE:** The “0” on the keypad is used to **delete** characters.

**Table 1: Data Entry at Keypad**

Key	Value	Key	Value	Key	Value
1	1-A-B-C	4	4-J-K-L	7	7-S-T-U
2	2-D-E-F	5	5-M-N-O	8	8-V-W-X
3	3-G-H-I	6	6-P-Q-R	9	9-Y-Z-0

### ENTERING ASCII CHARACTERS

To enter American Standard Code for Information Interchange (ASCII) characters at the keypad, perform the following:

1. Press [\*] and use [<] [>] keys to scroll to “ASCII Entry”.
2. Press [\*] to select ASCII entry mode.
3. Use the [<] [>] keys to scroll to display the ASCII character you want to use and press [\*] to accept.
4. Press [\*] to exit ASCII character entry mode and return to normal entry.

**NOTE:** Authorized access to Connect24 (3G2055/TL2553G) or DLS IV (TL255) is required to modify any Ethernet/Cellular Programming Section. Specific panel Sections must be configured for proper operation of the Communicator with the panel.

### MOUNTING CONSIDERATIONS

The Cellular/Ethernet Communicator is fixed, wall-mounted unit 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 it must be 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!**

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

- This manual shall be used in conjunction with the Alarm controller manual; All the safety instructions specified within that manual shall be observed. (or equivalent)
- 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 trained service personnel only.
- Use authorized accessories only with this equipment.

### Cellular Coverage for Alarm Communicator Operation

The HSPA/3G performance of the **3G2055** and **TL2553G** Alarm Communicators depends greatly on Cellular network coverage. The SCW (with internal Alarm Communicator) should not be mounted in the final location without first ensuring that Cellular radio reception is adequate for communication using the HSPA/3G paths. Perform the “Communicator Placement Test” on page 9.

## COMMUNICATOR TECHNICAL SPECIFICATIONS

### GENERAL INFORMATION

All versions of the HSPA/3G and Ethernet Alarm Communicator, operate on a HSPA/3G network and are housed inside the Self Contained Wireless (SCW) 9055/9057. The Communicators use an Internal Antenna only. (Author's Note: Underlined by Aun. 2clrfy. mm-0715-0841)

Each version of Alarm Communicators covered by this Installation Manual are described below:

**3G2055:** A High Speed Packet Access/Global System for Mobile (HSPA/3G) wireless 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 digital cellular network.

**TL2553G:** Is a dual-path Cellular/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 digital cellular network.

The dual path Communicator can be used as either a backup or primary Communicator. The Communicator supports Internet Protocol (IP) transmission of panel and internal events over Ethernet/Internet and/or HSPA/3G.

**TL255:** Is an Ethernet Alarm Communicator that send alarm communication to Sur-Gard System I, II, III, and IV central station receivers through Ethernet/Internet networks.

#### CAUTION:

- Do not stay close to the equipment during device operation and to do not touch any exposed wires and other conductive surfaces.
- Recycle the battery according to the local rules and regulations.

**NOTE:** Prior to installation of the **3G2055** or **TL2553G** Communicator, confirm with your local carrier that the HSPA/3G network is available and active in the area where the Communicator will be installed, and that the location provides a radio signal strength that is adequate for uninterrupted service.

### FEATURES

- 128-bit Advanced Encryption Standard (AES) encryption via HSPA/3G and Ethernet/Internet
- Activating, initializing and remote programming through Connect 24.
- Back up or primary HSPA/3G/2G alarm communication.
- Does not require an external HSPA/3G/2G antenna.
- Ethernet LAN/WAN 10/100 BaseT (TL2553G/TL255 only).
- Full event reporting to central station.
- Fully redundant Ethernet/Internet and HSPA/3G/2G Dual-path Alarm Communication (TL2553G only).
- Individual Ethernet and/or HSPA/3G Periodic test transmission.
- Integrated call routing.
- Panel remote uploading/downloading support via HSPA/3G and Ethernet/Internet.
- Quad-Band Operation: 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz.
- CID and SIA format reporting.
- Subscriber Identity Module (SIM) card included with Communicator. (NA only)
- Supervision heartbeats via HSPA/3G/2G and/or Ethernet/Internet.

### UL/ULC INSTALLATION REQUIREMENTS

- For ULC Residential fire and burglary applications the **3G2055/TL2553G/TL255** can be used as primary communication channel via either Cellular or Ethernet (as applicable) or as a back-up in conjunction with the Digital Alarm Communicator Transmitter (DACT). Test transmission every 24hours shall be enabled on each channel.
- For UL Residential fire and burglary applications the **3G2055/TL2553G/TL255** can be used as 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).

### COMMUNICATOR FREQUENCY BANDS FOR NORTH AMERICA

Table 2: 2G Frequency Bands

Transmit Direction	Cellular 850 North America	PCS 1900 North America
Transmit Frequency	824 MHz to 849 MHz	1850 MHz to 1910 MHz
Receive Frequency	869 MHz to 894 MHz	1930 MHz to 1990 MHz

Table 3: 3G Frequency Bands

Transmit Direction	UMTS 850 North America, International	UMTS 1900 North America
Transmit Frequency	824 MHz to 849 MHz	1850 MHz to 1910 MHz
Receive Frequency	869 MHz to 894 MHz	1930 MHz to 1990 MHz

## RATINGS

**Table 4: Communicator Electrical Ratings**

Model	3G2055 Cellular Only	TL2553G Ethernet and Cellular	TL255 Ethernet Only
Power Supply Ratings			
Input Voltage	3.5 / 3.9 / 4.2 VDC (min / NOM / MAX) from the SCW panel		
Current Consumption	75 mA	100 mA	75 mA
Standby Current (@ 3.7V)	75 mA	100 mA	75 mA
Alarm (Transmitting) Current	400 mA @ 3.7V during transmission		
Antenna Specifications			
Dual band Antenna	See Table 2 and Table 3		N/A
Environmental Specifications			
Operating Temperature	0°C - 49°C (32°F - 120°F)		
Humidity	5% ~ 85% relative humidity, non-condensing		
Mechanical Specifications			
Board Dimensions (mm)	109 x 110		
Weight (grams)	60	65	45

## HARDWARE COMPATIBILITY

**Table 5: Compatibility**

Communicator	Receiver/ Control Panel	Description
3G2055	Receiver	SG- System I V1.12 and newer
TL255		SG-System II , V2.02 and newer
TL2553G	Control Panel	SG-System IV (SG-DRL3IP) V2.21, and newer
		SG-System IV (SG-DRL3IP) V2.21, and newer
		SCW9055/SCW9057 V1.00

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.

## SOFTWARE COMPATABILITY

The Communicator is compatible with the following software:

- Connect24 Using: Simple Messaging System (SMS) Protocol.
- Connect24 Remote Flash. Using: Internet Protocol (IP) using Trivial File Transfer Protocol (TFTP).

## COMMUNICATOR PRE INSTALLATION CONFIGURATION

### CONNECT24™<sup>1</sup> ACCOUNT AND SIM CARD ACTIVATION

(Before Installation)

Installation of the Communicator requires activation with Connect24 before operation. Dealer application forms and additional information on the Connect24 Voice Response Unit (VRU) and graphical user interface (GUI) can be found at <http://www.Connect24.com> or by telephone at: USA 1-888-251-7458 or CANADA 1-888-955-5583.

**IMPORTANT:** Prior to installing a **3G2055**; **TL2553G**; or **TL255** Communicator, contact your monitoring station to determine if it is a master re-seller or visit <http://www.Connect24.com> to become an authorized dealer. In either instance, you will receive a Profile Number, Installer ID Number, and an Installer Password. Perform the following pre installation:

1. Retrieve the installer account and password from the master reseller, or from Connect24 directly.
2. Connect your browser to the Connect 24 website at: <http://www.Connect24.com> or call VRU number.
3. Log in to the Connect24 website using your installer account and password.
4. Perform the following steps in a Connect24 session to activate the SIM card and initialize programming:
  - a. Navigate to the **Initialize an account** section.
  - b. Select **Profile** (This information will be provided by the master reseller or by Connect24).
  - c. Select **Product** Module.
  - d. Enter the SIM card number.
  - e. Click **Next** then enter in all relevant information as required.
  - f. Confirm all information is entered correctly before submitting.
5. Repeat Step 4 to program another SIM card (i.e. another Subscriber), or log out from Connect24.
6. When you are at the physical installation site, the Communicator will automatically connect and download its programming from Connect24 once the unit is initialized.

1. **Connect24**, **DSC**, and **DLS IV** are Registered Trademarks of Tyco International Ltd. and its respective Companies. All Rights Reserved.

**NOTE:** Following initial installation, you can log in to the Connect24 website at any time to re-configure the Communicator remotely, using the account created for this installation. For more information, refer to the Connect24 website.

**Before leaving the installation site, the Communicator TL2553G or TL255 shall be connected via an APPROVED (acceptable to the local authorities) Network Interface Device (NID) (e.g., for UL Installations, U60950 listed NID). All wiring shall be performed according to the local electrical codes.**

**ENCRYPTION**

The Communicator uses 128 Bit AES Encryption. Encryption can only be enabled from the monitoring station receiver. Each receiver 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.

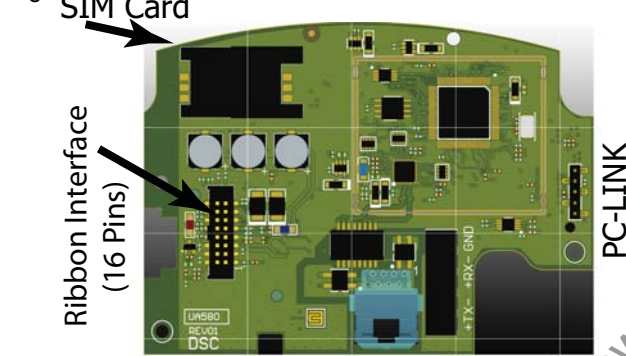
**NOTE:** Packets will start being encrypted only after the next event is sent to that receiver, or if the unit is restarted.

**COMMUNICATOR CONFIGURATION WITH SCW**

**NOTE:**

**NOTE:**

Figure 1: 11A580 PCB Connection Points



DG009640

**RJ-45**  
Use CAT 5 Cable Only

**NOTE:** The Alarm Communicator is installed in the SCW prior to shipment by Digital Security Controls (DSC). The Factory Installation includes insertion of the SIM card. The SCW should not be mounted in its final location without performing a Communicator Test to ensure adequate HSPA/3G coverage for the 3G2055 and TL2553G Alarm Communicators

**INSTALLATION LOCATION**

The Communicator shall be installed in an indoor location within the Self Contained Wireless (SCW) Control Panel, and near the main entrance, on the main floor of the dwelling or other preferred place.

This HSPA/3G/Ethernet Communicator shall be installed by Service Personnel only. (Service Person is defined as a person having the appropriate technical training and experience necessary to be aware of hazards to which that person may be exposed in performing a task and 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, over voltages

category II, in non-hazardous, indoor locations only. This manual shall be used with the Installation Manual of the alarm control panel which is connected to the HSPA/3G/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 CAT 5 CABLE (TL2553G/TL255 ONLY)**

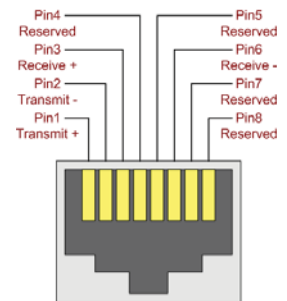
A Category 5 (CAT 5) ethernet cable must be run from a source with Ethernet/Internet connectivity to the Communicator module, inside the Self Contained Wireless Control Panel cabinet. The Communicator end of the cable must have an RJ-45 plug, which connects to the Communicator's RJ-45 jack. All requirements 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 1.2cm (1/2").
- 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 5 cm (2 in.) bend radius. Maximum length of CAT 5 cable is 100m (328 ft.).

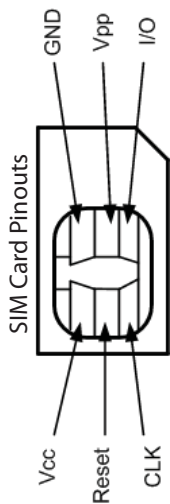
**NOTE:** The Ethernet cable shall not be visible when the installation is complete unless the install is a surface mount installation

Figure 2: RJ-45 Pinout



RJ-45 Connector  
DG0009635

Figure 3: SIM Card Pinouts



DG0009396

### INSERTING/REMOVING THE SIM CARD

1. Remove the front cover of the SCW Control Panel to access SIM card holder.
  2. Remove power from the SCW and disconnect the backup battery connections.
  3. On the SIM card holder push gently to slide the cover towards OPEN as indicated by the arrow on SIM holder. This will unlatch the SIM card holder on the side furthest from edge of the Communicator. See Figure 1.
  4. Lift up the SIM card holder from the side that is not hinged.
- NOTE:** The SIM card can be damaged by bending or scratching contacts. Use caution when handling the SIM card.
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. Apply AC power to panel, and replace the panel cover.

### COMMUNICATOR RESET

The Communicator can be reset by cycling the power on the SCW.

### ESTABLISHING A COMMUNICATION CHANNEL WITH THE SCW PANEL.

The Communicator interfaces to the SCW through a keyed 16 pin Ribbon cable. See Table 6. The key prevents incorrect connection of the ribbon connector to the SCW and Communicator. The pinout for the Ribbon Interface is provided in the Table below.

Table 6: Communicator Ribbon cable to SCW

Pin #	Signal	Pin #	Signal
1	PC-Link TX	2	PC-Link RX
3	GND	4	Vref
5	Vref	6	GND
7	AUD-OUT_N	8	AUD-OUT_P
9	AUD-IN_P	10	AUD-IN_N
11	GND	12	SI
13	GND	14	SO
15	GND	16	Wall Tamper

Establishing a communication channel between the Communicator and the SCW is critical to ensuring the desired operation of the two units. The following steps must be completed during the on-site installation. Program the following to ensure that the Communicator and the panel will work together as intended.

#### Initial Programming of Communicator and SCW

1. Enter [\*][8][Installer Code][Section Number] for panel programming. Record any values that are modified from their default, in the appropriate Programming Worksheets.

**NOTE:** When programming Toggle Options, the toggle is ON when the number is displayed and OFF when the number is not displayed. (e.g., [1 - - - 5 - - -]. Toggle Options 1 and 5 are ON, all others are OFF).

2. Panel Section [167] Cellular/Ethernet Interface Communications ‘Wait for ACK’: Program value as: **060** (seconds).
3. When the communicator is installed with the SCW panel, 4 telephone number are available to backup one another. You can set up these 4 telephone numbers to perform in one of two ways: Backup dialling or Alternate dialling.
  - a. **Backup dialling:** each of the 4 telephone numbers will make 5 dialling attempts in turn, before an FTC trouble is displayed on the keypad.
  - b. **Alternate dialling:** each telephone number makes 1 dialling attempt before moving on to the next number, cycling through each of the 4 numbers for a total of 5 times each. If all 4 numbers fail the 5 attempts,, an FTC trouble is displayed on the keypad.
4. Panel Sections [301], [302], [303], and [305] can be configured as Primary communication paths.
  - a. Panel Sections [302], [303], and [305] may also be configured for backup or redundant communications by using Panel Section(s) [383] or [351] - [376]. Refer to the SCW panel Installation Manual for more information.
  - b. If a valid telephone number is programmed, communications will use Public Switched Telephone Network (PSTN). Entering a 4 digit hexadecimal value for a telephone number will change the call routing to the Communicator, as determined by the number programmed:
    - DCAAF:** Internal (All Receivers). Signals will be routed depending on Section [851] [006] programming.
    - DCBBF:** Ethernet Receiver 1 (Primary). (Not available for 3G2055).
    - DCCCF:** Ethernet Receiver 2 (Backup). (Not available for 3G2055).
    - DCDDF:** Cellular Receiver 1 (Primary). (Not available for TL255).
    - DCEEF:** Cellular Receiver 2 (Backup). (Not available for TL255).

**NOTE:** Add a single ‘F’ as a suffix to the 4 digit hex number to populate the unused remainder of the 32 character field.

5. Panel Section [350]: If any of the phone numbers have been programmed as DCAA, DCBB, DCCC, DCDD, or DCEE, panel Section [350] must be set to [04] if SIA format or [03] if Contact ID (CID) format is used by control panel.



6. Panel Section [382]: Toggle Option [5], 'GS/IP Module Enabled', must be set to **ON**.
7. Panel Section [401]: Toggle Option [1] must be set to **ON** in order to perform panel DLS session through Cellular or Ethernet data channel.

**NOTE:** Keep a record of the SIM card telephone number, it is required by users for SMS Command and Control functions. (The number can be recorded in the Programming Worksheets Section of this document, under Option [996]) Due to the nature of the SIM card activation process with Cellular network carriers, it can take up to 24 hours for SIM card activation to be complete.

## LABEL PROGRAMMING FOR SMS MESSAGE

Programmable Labels can not be modified in Connect24, use DLS IV for label programming only, if labels need to be modified. Before initiating remote programming, record your network's Public IP Address and port for incoming DLS IV connections.

1. Run the DLS IV software on your computer. DLS IV will connect to the unit, using the Public IP address, and make an Ethernet connection. If the Ethernet connection fails, DLS IV will report an error and prompt you to connect using Cellular.

**NOTE:** If required, download the DLS IV software from DSC: <http://www.dsc.com/index.php?n=library#self>. If you select the Cellular connection, DLS will request Connect24 to send an outgoing SMS message to the unit.

2. Connect24 will confirm that the account has DLS service and will provide the Public IP address and port number of the DLS server in an SMS message.
3. Type the SMS message text into your cell phone and send it to the Communicator's Cellular telephone number. Click **OK**.

**NOTE:** The Cellular phone number can be read from Communicator Section [851][996].

4. SMS message will establish a connection to your computer's DLS IV software (to change programming labels only).
5. Create an account for the panel/Communicator, select the Communicator type (e.g., SMS - TL2553G) and enter all relevant information in **SMS** section.

**NOTE:** The Cellular telephone number will also be required by the user, to send SMS Interactive messages to their system.

6. Program the account information, then click **Global Download** and choose **SMS** as the **Connection Type**. Click **OK**.
7. The download path configured in Programming Section [005] Toggle Option [4] determines the Cellular or Ethernet path to be used.

## COMMUNICATOR PLACEMENT TEST

(3G2055/TL255GS only)

1. Using the [<] and [>] keys on the SCW keypad, scroll to the "Signal Strength Menu".
2. Press [\*] key to select Signal Strength mode.
3. View and record the number of bars showing on the SCW LCD.
4. Compare with the number of bars indicated in the "CSQ Levels" column shown in Table 7.
5. If 3 or more bars are shown, the location is GOOD and no further action is required.
6. If the location is BAD, move the SCW to various suitable locations until 3 or more bars are obtained.

**Table 7: Communicator CSQ Levels**

Signal Strength	CSQ Level	Signal Level dBm	Installer Action
No Signal	0	-108.8	Check if Cellular coverage is active in your area.
1 Bar	1 to 4	-108d to -103	Location is BAD. Not suitable for Cellular operation.
2 Bars	5 to 6	-102 to -99	Location is FAIR. If the average signal strength is CSQ is 5, the system may not communicate events successfully to the Monitoring Station. Installer should consider relocation, if possible
3 Bars	7 to 10	-98d to -91	Location is GOOD.
4 Bars	11 to 13	-90 to -85	Location is GOOD
5 Bars	14 and higher	-84 and higher	Location is GOOD.

## ETHERNET/CELLULAR PROGRAMMING OPTIONS

The Programming Sections described in this document can be viewed at the SCW 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.

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

### 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 passive systems (not using heartbeat supervision), 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.

**[005] System Toggle Options****[1] Ethernet Receiver 1 Supervised**

Default (OFF)

(TL255/TL2553G 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. (8 flashes on yellow trouble LED). (Author's Note: AH>MM: "Wherever we have text like this: "Supervisory trouble is indicated. (8 flashes on yellow trouble LED).", it is to be replaced with new text TBD> For now this text is just a 'placeholder'. mm-0715-0855)

**NOTE:** Ethernet Receiver 2 can not be supervised.

**[2] Cellular Receiver 1 Supervised** (Author's Note: m/n-0707-1627:FB,MM "We might replace need to use words **Radio/Wireless** instead of across entire document. mm-0715-1526)

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. (8 flashes on yellow trouble LED). (Author's Note: See mm-0715-0855 above, Pg-11.)

**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] Wireless Primary**

Default (OFF - TL255/TL2553G) (ON - 3G2055)

**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**

Default (OFF) (TL2553G only)

**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 the Cellular trouble event (5 flashes on Yellow Trouble LED).

**ON:** A Cellular Trouble event (5 flashes) is transmitted to receiver when the radio signal level falls below threshold level (average CSQ level is 5 or less).

**OFF:** A Cellular Trouble event (5 flashes) is **not** transmitted to receiver when the radio signal level falls below threshold level (average CSQ level is 5 or less). (Author's Note: See mm-0715-0855 above, Pg-11.)

**[006] System Toggle Options 2****[1] Ethernet 1 Receiver Enabled.**

Default (ON) (OFF for **3G2055**).

**ON:** Ethernet Receiver 1 is enabled.

**OFF:** Ethernet Receiver 1 is disabled.

**[2] Ethernet 2 Receiver Enabled.**

Default (ON) (OFF for **3G2055**).

**ON:** Ethernet Receiver 2 is enabled.

**OFF:** Ethernet Receiver 2 is disabled.

**[3] Reserved. (OFF).****[4] Cellular 1 Receiver Enabled.**

Default (ON).(OFF for **TL255**)

**ON:** Cellular Receiver 1 is enabled.

**OFF:** Cellular Receiver 1 is disabled.

**[5] Cellular 2 Receiver Enabled.**

Default (ON).(OFF for **TL255**)

**ON:** Cellular Receiver 2 is enabled.

**OFF:** Cellular Receiver 2 is disabled.

**[6] Reserved (OFF).****[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] Interactive over Cellular.**

Default (ON).

**[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****[010] 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. (Author's Note: m/n-0707-1627:FB,MM "We need to add option [010]. THIS IS PLACE HOLDER. mm-0715-1621)

**[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 configur-

ing 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.

### [020] 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. (Author's Note: m/n-0707-1627:FB,MM "We need to add option [010], THIS IS PLACE HOLDER. mm-0715-1632)

### [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: 000001-FFFFFFE. If 4 digit account codes are needed the 2 lowest digits shall be programmed as FF.

(e.g., Account 1234 is programmed as:1234FF).

**NOTE:** Programming this Section with all 0 or F will cause a Module Configuration Trouble (yellow LED=12 flashes). (Author's Note: See mm-0715-0855 above, Pg-11.)

### [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. Example: **Nri0 ET001**

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

## COMMUNICATIONS REPORTING CODES

**Table 8: 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].

**[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.

**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 heart-beat signals to the central station receiver. Signals received from the Panel will use the control panel account number. Valid range: 0000000001-FFFFFFFFFE. Programming all **0** or all **F** will cause a Module Configuration Trouble (yellow LED=12 flashes).

**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 - 099999. 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

**[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 heart-beat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid range: 0000000001-FFFFFFFFFE. 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 - 099999. 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 ( )

**D** 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 heart-beat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid range: 0000000001 - FFFFFFFF00. 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 - 099999. 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: 0000000001 - FFFFFFFF0E.

**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 - 099999. 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.

**NOTE:** This Section is not accessible via PC1616/PC1832/PC1864 keypad programming.

**[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: 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.

**[226] Cellular Trouble Delay**

Default (00)

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.

**[682] Notification Zone 1 - 8 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 11: Notification Zone 1 - 8 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	1	2	3	4	5	6	7	8

**[683] Notification Zone 9 - 16 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 12: Notification Zone 9 - 16 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	9	10	11	12	13	14	15	16

**[684] Notification Zone 17 - 24 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 13: Notification Zone 17 - 24 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	17	18	19	20	21	22	23	24

**[685] Notification Zone 25 - 32 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 14: Notification Zone 25 - 32 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	25	26	27	28	29	30	31	32

**[686] Notification Zone 33 - 40 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 15: Notification Zone 33 - 40 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	33	34	35	36	37	38	39	40

**[687] Notification Zone 41 - 48 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 16: Notification Zone 41 - 48 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	41	42	43	44	45	46	47	48

**[688] Notification Zone 49 - 56 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 17: Notification Zone 49 - 56 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	49	50	51	52	53	54	55	56

**[689] Notification Zone 57 - 64 Toggle Options**

The default for each Notification Zone Toggle is OFF.

**Table 18: Notification Zone 57 - 64 Toggle**

TOGGLE	01	02	03	04	05	06	07	08
ZONE	57	58	59	60	61	62	63	64

## 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.

## SYSTEM INFORMATION (READ ONLY)

**NOTE:** Sections [987] - [998] are provided for information (Read Only). Values in these Sections can not 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 unique 12 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.

29007850R001 \_ Shared \_ Review \_ updated \_ by \_ MM \_ 04

29007850R001 \_ Shared \_ Review \_ updated \_ by \_ MM \_ 04

## 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.

Default [OFF] TL2553G; [ON]3G2055.

[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.

\_\_\_\_\_

**Program your installer code for this Communicator module. The installer code will be required when programming the Communicator module. Valid range: 0000 - FFFF. (Author's Note: m/n-0707-1627:FB,MM "We need to add option [010]. THIS IS PLACE HOLDER. mm-0715-1632)**

Default (FFFFFF)

\_\_\_\_\_

**[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.

\_\_\_\_\_

### ETHERNET RECEIVER 1 OPTIONS

**[101] Ethernet Receiver 1 Account Code**

Default (0000000000)

Valid range: 0000000001 - FFFFFFFF0E.

\_\_\_\_\_

**[102] Ethernet Receiver 1 DNIS**

Default (000000) Valid range: 000000 - FFFFFFFF.

\_\_\_\_\_

**[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 - FFFFFFFF0E.

\_\_\_\_\_

**[112] Ethernet Receiver 2 DNIS**

Default (000000) Valid range: 000000 - 0FFFFFFF.

\_\_\_\_\_

**[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 - FFFFFFFF00.

\_\_\_\_\_

**[202] Cellular Receiver 1 DNIS**

Default (000000) Valid range: 000000 - 0FFFFFFF.

\_\_\_\_\_

**[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: 0000000001 - FFFFFFFF00.

\_\_\_\_\_

**[212] Cellular Receiver 2 DNIS**

Default (000000)

Valid range: 000000 - 0FFFFFFF.

\_\_\_\_\_

**[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 (00)

Program 00 disable or FF enable.

\_\_\_\_\_

**INTERACTIVE OPTIONS**

**[651] Interactive Account Code**

Default (MAC or IMEI)

\_\_\_\_\_

**[652] Interactive Access Code**

Default (1234)

\_\_\_\_\_

**[661] Interactive Baud Rate**

Default (05)

\_\_\_\_\_

**[662] Interactive Port Settings Toggle**

\_\_\_\_| [1] Parity Enabled Default (OFF).

\_\_\_\_| [2] Even/Odd Parity Default (OFF).

\_\_\_\_| [3] 1 or 2 Stop Bits Default (OFF).

\_\_\_\_| [4] Flow Control. Default (OFF).

**[681] Notification Event Toggle**

- [1] Alarm/Restore Default (OFF).
- [2] Tamper/Restore Default (OFF).
- [3] Opening/Closing Default (OFF).
- [4] System Maintenance. Default (OFF).
- [5] System Test Default (OFF).
- [6] Internal Events Default (OFF).

**[682] Notification Zone 1 - 8 Toggle Options**

\_\_\_\_\_

1 2 3 4 5 6 7 8

**[683] Notification Zone 9 - 16 Toggle Options**

\_\_\_\_\_

9 10 11 12 13 14 15 16

**[684] Notification Zone 17 - 24 Toggle Options**

\_\_\_\_\_

17 18 19 20 21 22 23 24

**[685] Notification Zone 25 - 32 Toggle Options**

\_\_\_\_\_

25 26 27 28 29 30 31 32

**[686] Notification Zone 33 - 40 Toggle Options**

\_\_\_\_\_

33 34 35 36 37 38 39 40

**[687] Notification Zone 41 - 48 Toggle Options**

\_\_\_\_\_

41 42 43 44 45 46 47 48

**[688] Notification Zone 49 - 56 Toggle Options**

\_\_\_\_\_

49 50 51 52 53 54 55 56

**[689] Notification Zone 57 - 64 Toggle Options**

\_\_\_\_\_

57 58 59 60 61 62 63 64

**RECEIVER DIAGNOSTIC TESTING**

**[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

\_\_\_\_\_

29007850R004 - Shared\_Review\_Updated - 2011-11-04

## 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-3G255SM

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

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 interférences 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.



29007850R001

---

**DSC**

*A Tyco International Company*

© 2011 Tyco International Ltd. and its Respective Companies. All Rights Reserved.  
Toronto, Canada · [www.dsc.com](http://www.dsc.com)  
Tech Support : 1-800-387-3630 (CA, US), 905-760-3000  
Printed in Canada