3G2055-SM-NA

HSPA/3G/2G Wireless Alarm Communicator

TL255-NA

Ethernet/Internet Alarm Communicator

TL2553G-SM-NA

Ethernet/Internet and HSPA/3G/2G Dual-Path Alarm Communicator

DRAFT-02_by_MM

DSC
A Tyco International Company

ULC · UL · ADT Security Systems

v3.0
Installation Manual

File Name: 29007848R001_Draft_updated_by_MM_DRAFT_02

TABLE OF CONTENTS

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, barbeques, 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

ⓘ **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-SM/TL2553G-SM) or DLS IV (TL255-SM) 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.

Technical Specifications

3G2055-SM: A HSPA/3G/2G 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/2G digital cellular network. The 3G2055-SM uses an internal antenna for radio coverage.

TL2553G-SM: A dual-path HSPA/3G/2G/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/2G 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/2G. The TL2553G-SM uses an internal antenna for radio coverage.

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

The HSPA/3G/2G performance of the **3G2055-SM** and **TL2553G-SM** Alarm Communicators depends greatly on HSPA/3G/2G network coverage. The unit should not be mounted in the final location without first ensuring that HSPA/3G/2G radio reception is adequate.

• Do not stay close to the equipment during device operation and to do not touch the antenna, (or equivalent) and,

• Recycle the battery according to the local rules and regulations.

NOTE: Prior to installation of the 3G2055-SM or TL2553G-SM Communicator, confirm with your carrier that the HSPA/3G/2G network is available and active in the area where the Communicator will be installed and that radio signal strength is adequate for uninterrupted service.

FEATURES

• 128-bit Advanced Encryption Standard (AES) encryption via HSPA/3G/2G and Ethernet/Internet.

• Activating, initializing and remote programming through Connect 24.

• Back up or primary 3G alarm communication.

• Does not require an external 3G antenna.

• Ethernet LAN/WAN 10/100 BaseT (TL2553G-SM/TL255-SM only).

• Full event reporting to central station.

• Fully redundant Ethernet/Internet and 3G Dual-path Alarm Communication (TL2553G-SM only).

• Individual Ethernet and/or Cellular Periodic test transmission.

• 2-way audio (listen-in feature) provided over Cellular and over the IP - *Dan Nita suggested it in his comments. Ask if the other manual needs this line and update other manual.*

• Integrated call routing.

• Panel remote uploading/downloading support via 3G and Ethernet/Internet.

• Programmable Labels (Zone and Partition Labels autosync with the panel.)

• 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-SM/TL2553G-SM/TL255-SM** can be used as primary communication channel via either HSPA/3G/2G 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-SM/TL2553G-SM/TL255-SM** can be used as primary communication channel via either HSPA/3G/2G or Ethernet, or as a back-up in conjunction with the DACT. (30 day test transmission is required on each channel).

RATINGS

Table 2: Communictor Electrical Ratings

Model	3G2055-SM Cellular Only	TL2550GS Ethernet and Cellular	TL255-SM 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
Current Consumption	75 mA	100 mA	75 mA

Table 3: Quad Band Antenna Frequencies

Transmit Direction	ECellular 900 International	DCS 1800 International	Cellular 850 North America	PCS 1900 North America
TX Frequency	880 ~ 915 MHz	1710 ~ 1785 MHz	824 ~ 849 MHz	1850 ~ 1910 MHz
RX Frequency	925 ~ 960 MHz	1805 ~ 1880 MHz	869 ~ 894 MHz	1930 ~ 1990 MHz

HARDWARE COMPATIBILITY

Table 4: Compatibility

Communicator	Receiver/ControlPanel	Description
3G2055-SM TL255-SM-NA TL2553G-SM	Receiver	Sur-Gard System I Receiver, version 1.10+ Sur-Gard System II Receiver, version 2.00+ Sur-Gard DRL3IP, version 2.20+ Sur-Gard DRL4IP, version 1.10+
	Control Panel	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. 950-1 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 SMS Protocol).
• Connect24 Remote Flash. (IP using TFTP).
• System Administrator.

Communicator Pre Installation Configuration

CONNECT24™[1] 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-SM/TL2553G-SM/TL255-SM 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.

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-SM/TL255-SM 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 Installation

INSTALLATION LOCATION

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

This 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 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-SM/TL255-SM 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 RJ45 plug, which connects to the Communicator's RJ45 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 (½").

• 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. Do NOT exceed maximum 15cm (6 in.) from center of ferrite to T-Link Network Connector. Maximum length of CAT 5 cable is 100m (328 ft.).

---

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

INSERTING THE SIM CARD

1. Remove the front cover of the SCW Control Panel to access SIM holder.

2. Power down the panel 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.

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.

Figure 1:   Layout of UA580

HARDWARE RESET

The Communicator can be hardware reset by installing a jumper between Pins 4 and 5 on the AUDIO/DEFAULT connector.

ESTABLISHING A COMMUNICATION CHANNEL WITH THE SCW PANEL.

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 followingto ensure that the Communicator and the panel will work together as intended.

NOTE: Panel Sections must be programmed at the panel keypad.

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-SM).
   DCCCF: Ethernet Receiver 2 (Backup). (Not available for 3G2055-SM).
   DCDDF: Cellular Receiver 1 (Primary). (Not available for TL255-SM-NA).
   DCEEF: Cellular Receiver 2 (Backup). (Not available for TL255-SM-NA).

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.

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.

NOTE: Keep a record of the SIM card telephone number, it is required by users for SMS Command and Control functions. Due to the nature of the SIM card activation process with 3G network carriers, it can take up to 24 hours for SIM card activation to be complete.
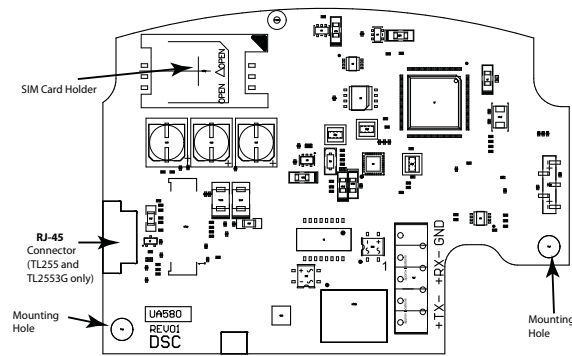
LABEL PROGRAMMING for SMS MESSAGES

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.Type the SMS message text into your cell phone and send it to the Communicator's 3G telephone number. Click **OK**.

NOTE: The 3G phone number can be read from Communicator Section **[851][996]**.

3. SMS message will establish a connection to your computer's DLS IV software (to change programming labels only).

4. Create an account for the panel/Communicator, select the Communicator type (e.g., SMS - TL2553G-SM) and enter all relevant information in **SMS** section.

NOTE: The 3G telephone number will also be required by the user, to send SMS Interactive messages to their system.

5. Program the account information, then click **Global Download** and choose **SMS** as the **Connection Type**. Click **OK**.

6. The download path configured in Programming Section **[005]** Toggle Option[4] determines the Cellular or Ethernet path to be used.

ETHERNET/Cellular Programming Options

The Programming Sections described in this document can be viewed through the panel Section for Ethernet/Cellular 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); (**TL255-SM/TL2553G-SM only**)
Enter the IP address of the dual 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); (**TL255-SM/TL2553G-SM only**)
Enter the Ethernet IP Subnet Mask of the dual Communicator. 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 subnet mask for this Section and the programmed value will be ignored.

[003] Ethernet Gateway IP Address
Default (000.000.000.000); (**TL255-SM/TL2553G-SM only**)
Enter the Ethernet Gateway IP address of the dual 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 communication path. Use this Section to set the interval time (in seconds) when heartbeats will be sent. Valid range 000A-FFFF seconds. If the programmed value is less than (000A/10) seconds, supervision is disabled.

Table 5: Receiver Supervision Intervals

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

- **Receiver Window**: This is the supervision timeout that needs to be configured at the central station receiver.
- **Recommended Values**: This is the recommended heartbeat interval that should be programmed into the Communicator module.
- For ULC passive systems (not using heartbeat supervision), the daily test transmission must be enabled over each available communication channel Section [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-SM-NA/TL2553G-SM only).

   ON: Ethernet Receiver 1 will be supervised and heartbeats will be sent to Ethernet Receiver 1 based on the supervision interval programmed in Section [004].
   OFF: Ethernet Receiver 1 will not be supervised. When disabled, heartbeat 1 is sent to the Ethernet receiver once every hour, regardless of supervision type (heartbeat 1 or 2). The heartbeat is resent every 5 seconds until ACK. If no event or heartbeat ACK is received after (Receiver Supervision Interval + 75 seconds), Supervisory trouble is indicated.

NOTE: Ethernet Receiver 2 can not be supervised.

[2] Cellular Receiver 1 Supervised
   Default (OFF)

(3G2055-SM/TL2553G-SM only)

   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.
   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] Cellular Primary
   Default (OFF - **TL255-SM/TL2553G-SM**) (ON - **3G2055-SM**).

   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.
   NOTE: When the Communicator receives a Short Message Service (SMS) request to connect to Downloading Software (DLS), it will always use the primary path first to connect to DLS. If the primary path fails, it will use the secondary path.

[5] Redundant Communications
   Default (OFF)

(TL2553G-SM 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.
   NOTE: This Toggle should be OFF for applications where 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] Reserved. Default (OFF).

[006] System Toggle Options 2

[1] **Ethernet 1 Receiver Enabled.** Default (ON) [OFF **3G2055-SM**].
   ON: Ethernet Receiver 1 is enabled.
   OFF: Ethernet Receiver 1 is disabled.

[2] **Ethernet 2 Receiver Enabled.** Default (ON) [OFF **3G2055-SM**].
   ON: Ethernet Receiver 2 is enabled.
   OFF: Ethernet Receiver 2 is disabled.

[3] Reserved. (OFF).

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

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

[6] Reserved (OFF).

[7] **DLS Over Cellular.** Default (**ON**). [OFF **TL255-SM**]
   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 Toggle Option [7] is OFF, DLS sessions will occur on the Ethernet path only, regardless of Primary Path set in Section [005] Toggle Option [4]. If it is ON then the Communicator will connect to the primary path first for DLS and if the session fails, the secondary path will be used.

[8] **Reserved.** 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.

[009] Language

Default (01);

Table 6: Label Languages

OPT	Language	OPT	Language	OPT	Language	OPT	Language
00	**Reserved**	08	Czech	16	Turkish	24	Lithuanian
01	English	09	Finnish	17	**Reserved**	25	Ukrainian
02	Spanish	10	German	18	Croatian	26	Slovakian
03	Portuguese	11	Swedish	19	Hungarian	27	Serbian
04	French	12	Norwegian	20	Romanian	28	Estonian
05	Italian	13	Danish	21	Russian	29	Slovenian
06	Dutch	14	Hebrew	22	Bulgarian	30-99	**Reserved**
07	Polish	15	Greek	23	Latvian		

NOTE: Immediately after programming this Section, perform a Default Languages in Section **[999][11]** to have programmable labels available in the selected language. Programming this Section with an invalid language number will default to English [01]. Connect24 will automatically update all programmable language labels when this Section is changed.

[010] System Toggle Options 3

Default (OFF)

[1]   Two way Audio over Cellular.

ON: Two way audio over the Cellular Voice channel is enabled.

OFF: Two way audio over the Cellular Voice channel is disabled.

[2]-[8] Reserved. Default (OFF)

PROGRAMMING OPTIONS

[011] Installer Code

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

[012] DLS Incoming Port

Default (0BF6/3062);
The DLS Incoming Local Port (listening port) is the port DLS IV will use when connecting to the Communicator. If a router or gateway is used, it must be programmed with a Transmission Control Protocol (TCP) port forward for this port to the Communicator module IP address. Valid range: 0000-FFFF.

[013] DLS Outgoing Port

Default (0BFA/3066);
The DLS Outgoing Port is used for outgoing session to DLS IV after an SMS request has been sent to the Communicator. Use this Section to set the value of the local outgoing port. The value must be changed if the Communicator is located behind a firewall and must be assigned a particular port number, as determined by your network administrator. In most cases, changing the default value or configuring your firewall with this port is not required. Valid range: 0000-FFFF.

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

[020] Time Zone

Default (00)
Use Column 2 (Offset Hours) to find your local Time Zone. Record the two digit HEX value from Column 1 (HEX Value) on the same row. Program this HEX value for your Time Zone. Valid range is 00 - FF.

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
01	-12	BIT	Baker Island Time	47	5.5	IST	Indian Standard Time
05	-11	NUT	Niue Time	48	5.75	NPT	Nepal Time
		SST	Somoa Standard Time	49	6	XJT	Xinjiang Standard Time
09	-10	HAST	Hawaii-Aleutian Standard Time			EKST	East Kazakhstan Standard Time
		THAT	Tahiti Time			LKT	Sri Lanka Time
		TKT	Tokelau Time			VOST	Vostok Time
		CKT	Cook Island Time			OMSK	Omsk Standard Time
0B	-9.5	MIT	Marquesas Island Time			NOVT	Novosibirsk Time
0D	-9	AKST	Alaska Standard Time			BTT	Bhutan Time
		GIT	Gambier Island Time			BIOT	British Indian Ocean Time
11	-8	PST	Pacific Standard Time	4B	6.5	CCT	Cococ Islands Time
		PST	Pitcarirn Standard Time			MMT	Myanmar Time
		CIST	Clipperton Island Standard Time	4D	7	CXT	Christmas Island Time
15	-7	MST	Mountain Standard Time			KOVT	Khovd Time
19	-6	CST	Central Standard Time			KRAT	Krasnoyarsk Time
		GALT	Galapagos Time			WIB	Waktu Indonesia Bagian Barat
		PIT	Peter Island Time			ICT	Indochina Time
		EAST	Easter Island Standard Time			BDT	Bangladesh Standard Time

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
1D	-5	EST	Eastern Standard Time	51	8	AWST	Australian Western Standard Time
		COT	Colombia Time			CST	China Standard Time
		ECT	Ecuador Time			HKST	Hong Kong Standard Time
		PET	Peru Time			WITA	Waktu Indonesia Bagian Tengah
		ACT	Acre Time			TWT	Taiwan Time
1F	-4.5	VST	Venezuela Standard Time			SST	Scarborough Shoal Time
21	-4	AST	Atlantic Standard Time			SIT	Spratly Island Time
		CLST	Chile Standard Time			SGT	Singapore Time
		BWST	Brazil Western Standard Time			PST	Philippine Standard Time
		SLT	San Luis Time			PIT	Pratas Islands
		PYT	Paraguay Time			PIT	Parcel Island Time
		JFST	Juan Fernandez Island Standard Time			MYT	Malaysia Time
		GYT	Guyana Time			MNT	Mongolia Time
		FKST	Falkland Island Standard Time			MBT	Macclesfield Bank Time
		BOT	Bolivia Time			IRKT	Irkutsk Time
23	-3.5	NST	Newfoundland Standard Time			BDT	Brunei Time
25	-3	CGT	Central Greenland Time			ACIT	Ashmore and Cartier Island Time
		ART	Argentina Time	52	8.25	APO	Apo Island Time
		BRT	Brazilia Time	54	8.75	ACWST	Australian Central Western Standard Time
		UYT	Uruguay Standard Time	55	9	YAKT	Yakutsk Time
		SRT	Suriname Time			JST	Japan Standard Time
		ROTT	Rothera Time			KST	Korea Standard Time
		PMST	St. Pierre & Miquelon Standard Time			WIT	Waktu Indonesia Bagian Timur
		GFT	French Guiana Time			TPT	East Timor Time
29	-2	GST	South Georgia and the South Sandwich Islands			PWT	Palau Time
		BEST	Brazil Eastern Standard Time	57	9.5	ACST	Australian Central Standard Time

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
2D	-1	EGT	Eastern Greenland Time	59	10	AEST	Australian Eastern Standard Time
		CVT	Cape Verde Time			GST	Guam Standard Time
		AZOST	Azores Standard Time			YAPT	Yap Time
31	0	WET	Western Europian Time			VLAT	Vladivostok Time
		GMT	Greenwich Mean Time (**UTC**)			TRUT	Truk Time
		SLT	Sierra Leone Time			PGT	Papua New Guinea Time
		IST	Ireland Standard Time			DTAT	District de Terre Adelie Time
35	1	CET	Central Europian Time			ChST	Chamorro Standard Time
		WAT	Western Africa Time	5B	10.5	LHST	Lord Howe Standard Time
		BST	British Summer Time	5D	11	KOST	Kosare Standard Time
39	2	EET	Eastern Europian Time			NCT	New Caledonia Time
		CAT	Central Africa Time			VUT	Vanuatu Time
		SYT	Syrian Standard Time			SBT	Solomon Island Time
		SAST	South Africa Standard Time			PONT	Phonpei Standard Time
		IST	Israel Standard Time			MAGT	Magadan Island Time
3D	3	MSK	Moscow Standard Time	5F	11.5	NFT	Norfolk Island Time
		EAT	Eastern Africa Time	61	12	NZST	New Zealand Standard Time
		AST	Arabic Standard Time			FJT	Fiji Time
		AST	Arabia Standard Time			WFT	Wallis and Futuna Time
		AST	Al Manamah Standard Time			TVT	Tuvalu Time
3F	3.5	IRST	Iran Standard Time			PETT	Petropavlovsk Time
41	4	AMST	Armenia Standard Time			NRT	Nauru Time
		SCT	Seychelles Time			MHT	Marshall Island Time
		GST	Gulf Standard Time			GILT	Gilbert Island Time
		SAMT	Samara Time			ANAT	Anadyr Time
		RET	Reunion Time	64	12.75	CHAST	Chatham Island Standard Time
		MUT	Mauritius Time	65	13	PHOT	Phoenix Island Time
		ICT	Iles Crozet Time			TOT	Tonga Time
		GET	Georgia Standard Time	69	14	LINT	Line Island Time
		AZT	Azerbaijan Time	70 - FF	N/A		Reserved
43	4.5	AFT	Afghanistan Time				

Table 7: World Wide Time Zones

HEX Value	Offset Hours	Std Abbrev	Location	HEX Value	Offset Hours	Std Abbrev	Location
45	5	CAST	Chinese Atlantic Standard Time				
		WKST	West Kazakhstan Standard Time				
		PKT	Pakistan Time				
		YEKT	Yekaterinburg Time				
		UZT	Uzbekistan Time				
		TMT	Turkmenistan Time				
		TJT	Tajikistan Time				
		TFT	French Southern and Antarctic Time				
		MVT	Maldives Time				
		MAWT	Mawson Time				
		KGT	Kyrgyzstan Time				
		HMT	Heard and McDonald Island Time				
		DAVT	Davis Time				

[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-FFFFFE. If 4 digit account codes are needed the 2 lowest digits shall be programmed as FF;(e.g., Account 1234 is programmed as:1234FF). Programming this Section as all 0 or all F will cause a Module Configuration Trouble (yellow LED=12 flashes).

[022] Communications Format

Default (04);

Program 03 for Contact ID (CID). Program 04 for SIA. Communicator will synchronize with the panel and use the same communication format as the panel regardless of the value set in this Section.

The module can be configured to send internal 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: **Nri0 ET001**

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

COMMUNICATIONS REPORTING CODES

Table 8: Event 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] Ethernet1 Test Transmission	RP	001	1	6	A3	951
[027] Ethernet2 Test Transmission	RP	002	1	6	A3	952
[028] Cellular1 Test Transmission	RP	003	1	6	A3	955
[029] Cellular2 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) and Section [027] to (00). Set Cellular Section [028] to (FF) and Section [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) and Section [027] to (FF). Set Cellular Section [028] to (FF) and Section [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: 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 or FF to enable. This event will occur when an FTC Trouble on the system restores.

[031] Panel Tamper Alarm

Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when a Panel Tamper occurs on the system.Setting this option to 00 will disable monitoring of the tamper switch. See Table 12 for SIA and CID reporting codes.

Table 9: Panel Tamper Reporting Codes

Event	SIA Identifier	SIA Reporting Code	CID Qualifier	CID Event Code	CID Reporting Code	CID User/ Zone
Panel Tamper	ES	001	1	1	45	001
Panel Tamper Restore	EJ	001	3	1	45	001

[032] Panel Tamper Alarm Restore

Default (FF);
Program 00 to disable this event transmission or FF to enable. This event will occur when a Panel Tamper event on the system restores. See Table 9 for SIA and CID reporting codes.

ETHERNET RECEIVER 1 OPTIONS

(TL255-SM/TL2553G-SM only)

[101] Ethernet Receiver 1 Account Code

Default (0000000000);
The account code is used by the central station to distinguish between transmitters. This account code is used when transmitting heartbeat signals to the central station receiver. Signals received from the control panel will use the control panel account number. Valid range: 0000000001-FFFFFFFFFE. Programming this Section as 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 Dialled 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/Cellular.

[104] Ethernet Receiver 1 Remote Port

Default (0BF5/3061);
This Section determines the remote port of Ethernet receiver 1. Valid range: 0000 - FFFF.

[105] Ethernet Receiver 1 Local Port

Default (0BF4/3060);
Use this Section to set the value of the local outgoing port. Set the value of this port when your installation is located behind a firewall and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

[106] Ethernet Receiver 1 Domain Name

Default ( );
Enter the Domain Name as 32 ASCII characters.
ⓘProgramming this Section is not permitted on a UL/ULC listed system.

ETHERNET RECEIVER 2 OPTIONS

(TL255-SM/TL2553G-SM only)

[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 this Section as 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 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 the same receiver.

[114] Ethernet Receiver 2 Remote Port

Default (0BF5/3061);
This Section is used to program the port number used by Ethernet Receiver 2. Set the value of this port when your installation is located behind a firewall, and must be assigned a particular port number as determined by your central station system administrator. Valid range: 0000 - FFFF.

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

[115] Ethernet Receiver 2 Local Port

Default (0BF9/3065);
Use this Section to program the value of the local outgoing port. You can set the value of this port when your installation is located behind a firewall and must be assigned a particular port number as determined by your network administrator. Valid range: 0000 - FFFF.

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

[116] Ethernet Receiver 2 Domain Name

Default (   );
ⓘProgramming this Section is not permitted on a UL/ULC listed system.
Enter the Domain Name as 32 Character ASCII.

ETHERNET OPTIONS

(TL255-SM-NA/TL2553G-SM only)

[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 10: Ethernet Test Transmission Interval

Test Transmission Interval	Daily	Weekly	Monthly
Programmed Minutes	001440	010080	043200

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

CELLULAR RECEIVER 1 OPTIONS

(3G2055-SM/TL2553G-SM only)

[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 - FFFFFFFFFE. Programming this Section as 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 five digits. 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: 0001 - FFFF.

NOTE: Programming a value of 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

(3G2055-SM/TL2553G-SM only)

[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 control panel will use the control panel account number. Valid range: 0000000001 - FFFFFFFFFE. Programming this Section as all 0 or all 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

(3G2055-SM/TL2553G-SM only)

[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 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 here. Format is up to 32 ASCII characters.

[223] Cellular Login Password

Default ( );

Some network carriers require you to provide login credentials when connecting to an APN. Program your login password here. 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 11: Cellular Test Transmission Interval

Test Transmission Interval	Daily	Weekly	Monthly
Programmed Minutes	001440	010080	043200

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

[226] Cellular Trouble Delay

Default (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 delay if value is programmed as 00.

[227] Voice Call Timeout

Default (00);
This option sets the Voice Call Timeout, in minutes. Programming a value of 00 will disable timeout. Valid range is 00 to FF.

[228] Voice Call Back Time

Default (0A);
This option sets the Voice call back time, in minutes. When the Communicator requests Call Back from the receiver, it will answer incoming calls during the programmed timeout period. If an incoming call is received after the timeout from requesting call back, the Communicator will answer the call and immediately hang up. Programming a value of 00 will disable timeout (accept all incoming calls). Default value is 0A/10 seconds. Valid range is 00 to FF.

[229] Voice Call Back Number

Default (SIM Telephone Number);
This option sets the Voice Call Back Telephone Number for the receiver. This number is used for Two Way calling. Current SIM telephone number can be viewed in Section [996]. Valid entry is 32 character ASCII.

EVENT NOTIFICATION AND INTERACTIVE OPTIONS

[301] Command and Control Toggle Options

  [1] SMS Notification Default (**ON**).
  [2] Reserved Default (**OFF**).
  [3] SMS Command and Control Default (**ON**).
  [4] Interactive Default (**ON**).
  [5] SMS Character Format Default (**See Table 12 below for default by language selection**).
       ON: SMS Unicode, maximum message length is 70 characters.
       OFF: 7 bit SMS, maximum message length is 160 characters.
  [6] Long SMS Message Handling Default (**OFF**);
       ON: If longer than maximum message length, it is split and sent as multiple SMS messages.
       OFF: If longer than maximum message length. A single, truncated SMS message is sent.
  [7-8]Reserved Default (**OFF**).

Table 12: Event Notification Language

Language	Default	Language	Default	Language	Default	Language	Default
English	OFF	Czech	ON	Greek	ON	Latvian	OFF
Spanish	OFF	Finnish	OFF	Turkish	OFF	Lithuanian	OFF
Portuguese	OFF	German	OFF	Croatian	ON	Ukrainian	ON
French	OFF	Swedish	OFF	Hungarian	ON	Slovakian	OFF
Italian	OFF	Norwegian	OFF	Romanian	OFF	Serbian	ON
Dutch	OFF	Danish	OFF	Russian	ON	Estonian	OFF
Polish	ON	Hebrew	ON	Bulgarian	ON	Slovenian	OFF

[311] - [318] SMS Phone Number 1 - 8

Default ( );
These Sections may be programmed through DLS IV or the keypad. Up to 8 SMS telephone numbers (4 - 32 digits) can be programmed in Section [31x] Where x is an SMS telephone number from 1 to 8. Leaving programming blank for a telephone number will disable that number. The User can program their own mobile telephone numbers at the keypad using
[*] [6] <> "SMS Programming". The SMS Command and Control feature utilize the SMS messaging service provided by the Cellular network and is subject to the limitations of SMS messaging. These limitations include delayed messages and lack of guaranteed delivery.

NOTE: SMS Command and Control (Sections [601] - [618] will only process messages from the mobile telephone numbers programmed in this Section if SMS Command and Control is enabled [301][3] ON. SMS responses are listed in Sections [621] - [630]. A blank telephone number is disabled.

SMS NOTIFICATION

[321] - [328] SMS Phone Number 1 - 8 Toggle Options

The toggles in this Section determine the type of event message that will be sent to the SMS number programmed in Sections [311] - [318].
  [1] SMS Notification Alarm/Restore   Default (ON).
  [2] SMS Notification Tamper/Restore   Default (ON).
  [3] SMS Notification Opening/Closing   Default (ON).
  [4] SMS Notification System Maintenance Default (ON).
  [5] SMS Notification System Test   Default (ON).
  [6] SMS Notification Internal Events   Default (ON).
  [7] SMS Notification Enabled   Default (ON).

[8] SMS Command and Control Enabled Default (ON).

NOTE: Each telephone number can be programmed to receive different event notifications. When more than 1 number receives the event, the system will send the message to phone number 1 first. Only 1 send attempt is made for each programmed number. Notification, for each programmed telephone number can be enabled/disabled with Toggle Option [7].

AREA LABEL PROGRAMMING

Each Area label is up to 32 ASCII characters, including spaces. The label language is specified in Section [009].

[351] Account Label

Default (Security System);
The Account Label is up to 32 ASCII characters. It is sent at the beginning of every SMS message originating from the Communicator module.This label is used to identify the system to the recipient of the SMS message.

[352] System Label

Default (System Area);
The System Label is up to 32 ASCII characters. It is used for notification messages that apply to the system.

NOTE: On single partition systems the System Label may be used for all messages.

[353] - [360] Partition 1- 8 Label

Default (Partition x);
Where x is a partition number from 1 - 8. Partition Labels are up to 32 ASCII characters. Labels are used for SMS notification messages that apply to a specific partition on the system.

USER LABEL PROGRAMMING

[361] - [400] User 1 - 40 Label

Default (User x);
Where x is the User number from 1 - 40. User labels are used to identify a User for SMS notification messages that apply to a specific user. There are 40 programmable User Labels. Each label is up to 16 ASCII characters. The label language is specified in Section [009].

ZONE LABEL PROGRAMMING

[401] - [464] Zone 1 - 64 Label

Default (Zone n);
Where n is a Zone number from 1 - 64. Zone Labels are up to 32 ASCII characters. Labels are used to identify the Zone for notification messages that apply to a specific Zone. The label language is specified in Section [009]. Zone labels are numbered 1 - 64 and Zones are numbered 1-128. No labels are assigned to Zones 65-128.

PANEL EVENT LABEL PROGRAMMING

[501] - [580] Event Labels

Default (see **Default Label** in Table 13);
There are 80 programmable Event labels. Each label is pre programmed with the default text shown in Table 13 .
Each label is up to 32 ASCII characters (including spaces). The language is specified in Section [009].

Table 13: Panel Event Labels

Event [Section] Label	Default Label	Event [Section] Label	Default Label
[501] Burglary Alarm	[Burglary Alarm]	[502] Burglary Alarm Restore	[Burglary Alarm Restore]
[503] Fire Alarm	[Fire Alarm]	[504] Fire Alarm Restore	[Fire Alarm Restore]
[505] 24 Hour Alarm	[24 Hour Alarm]	[506] 24 Hour Alarm Restore	[24 Hour Alarm Restore]
[507] Holdup Alarm	[Holdup Alarm]	[508] Holdup Alarm Restore	[Holdup Alarm Restore]
[509] Gas Alarm	[Gas / Carbon Monoxide Alarm]	[510] Gas Alarm Restore	[Gas / Carbon Monoxide Restore]
[511] Heat Alarm	[High Temperature Alarm]	[512] Heat Alarm Restore	[High Temperature Alarm Restore]
[513] Medical Alarm	[Medical Alarm]	[514] Medical Alarm Restore	[Medical Alarm Restore]
[515] Panic Alarm	[Panic Alarm]	[516] Panic Alarm Restore	[Panic Alarm Restore]
[517] Emergency Alarm	[Emergency Alarm]	[518] Emergency Alarm Restore	[Emergency Alarm Restore]
[519] Sprinkler Alarm	[Sprinkler Alarm]	[520] Sprinkler Alarm Restore	[Sprinkler Alarm Restore]
[521] Water Level Alarm	[Water Level Alarm]	[522] Water Level Alarm Restore	[Water Level Alarm Restore]
[523] Freeze Alarm	[Low Temperature Alarm]	[524] Freeze Alarm Restore	[Low Temperature Alarm Restore]
[525] Fire Supervisory	[Fire Supervisory]	[526] Fire Supervisory Restore	[Fire Supervisory Restore]
[527] Zone Tamper	[Zone Tamper]	[528] Zone Tamper Restore	[Zone Tamper Restore]
[529] Zone Fault	[Zone Fault]	[530] Zone Fault Restore	[Zone Fault Restore]

Table 13: Panel Event Labels

Event [Section] Label	Default Label	Event [Section] Label	Default Label
[531] Fire Trouble	[Fire Trouble]	[532] Fire Trouble Restore	[Fire Trouble Restore]
[533] Module Supervisory	[Module Supervisory Trouble]	[534] Module Supervisory Restore	[Module Supervisory Restore]
[535] General System Tamper	[General System Tamper]	[536] General System Tamper Restore	[General System Tamper Restore]
[537] Wireless Device Low Battery	[Wireless Device Low Battery]	[538] Wireless Device Low Battery Restore	[Wireless Device Battery Restore]
[539] Cross Zone/Police Code	[Burglary Verified]	[540] Burglary Not Verified	[Burglary Not Verified]
[541] Duress Alarm	[Duress Alarm]	[542] Opening After Alarm	[Disarmed After Alarm]
[543] Recent Closing	[Alarm Occurred After Arming]	[544] Alarm Canceled	[Alarm Canceled]
[545] Keypad Lockout	[Keypad Lockout]	[546] Exit Fault	[Exit Fault]
[547] Partial Closing	[Armed With Zones Bypassed]	[548] Zone Bypass	[Zone Bypassed]
[549] Zone Unbypass	[Zone Unbypassed]	[550] Auto Arm Cancel	[Automatic Arming Cancelled]
[551] Closing	[Armed By]	[552] Opening Label	[Disarmed By]
[553] Special Closing	[Armed]	[554] Special Opening	[Disarmed]
[555] Late to Open	[Late to Open]	[556] Delinquency	[Delinquency]
[557] General System Trouble	[General System Trouble]	[558] General System Trouble Restore	[General System Trouble Restore]
[559] AC Line Trouble	[AC Power Failure]	[560] AC Line Trouble Restore	[AC Power Restore]
[561] Battery Trouble	[Battery Trouble]	[562] Battery Trouble Restore	[Battery Restore]
[563] Bell Circuit Trouble	[Bell Circuit Trouble]	[564] Bell Circuit Trouble Restore	[Bell Circuit Restore]
[565] Auxiliary Power Trouble	[Auxiliary Power Trouble]	[566] Auxiliary Power Trouble Restore	[Auxiliary Power Restore]
[567] Ground Fault	[Ground Fault Trouble]	[568] Ground Fault Restore	[Ground Fault Restore]
[569] TLM Failure	[Telephone Line Failure]	[570] TLM Failure Restore	[Telephone Line Restore]
[571] FTC Trouble	[Fail To Communicate Trouble]	[572] FTC Restore	[Fail To Communicate Restore]
[573] Event Buffer 75% Full	[Event Buffer Near Full]	[574] DLS Lead In	[Remote Programming Begin]
[575] DLS Lead Out	[Remote Programming End]	[576] Installer Lead In	[Local Programming Begin]
[577] Installer Lead Out	[Local Programming End]	[578] Walk Test Lead In	[Walk Test Begin]
[579] Walk Test Lead Out	[Walk Test End]	[580] System Test	[System Test Message]

COMMUNICATOR EVENT LABEL PROGRAMMING

Table 14: Communicator Event Label

Event Section Label	Default Label	Event Section Label	Default Label
[591] Panel Absent Trouble	[Panel Communications Trouble]	[592] Panel Absent Trouble Restore	[Panel Communications Restored]
[593] Module Reprogramming	[Communicator Programming Updated]	[594] Firmware Update	[Communicator Firmware Updated]

SMS COMMAND AND CONTROL FUNCTIONS

Users can send SMS text messages from their mobile phone to the Cellular phone number assigned to their system. Commands are only accepted from telephone numbers that have been programmed in Sections [311]-[318]. The system will reject messages sent from telephone numbers that are not on the programmed list.

When the received SMS text matches a valid Section message, the function is performed on the control panel. Text messages are not case sensitive and extra spaces are ignored. A User Access Code may be required for some SMS messages.

The User can send just the partition number or the complete label.(e.g., "Away arm Partition 2 1234" is treated the same as "away arm 2 1234 ").

The SMS Message format is in 3 parts: **Command**, **Partition Label** (or only the partition number), and **Access Code**.

- If an Access Code is included in the message, it is sent to the control panel for validation, along with the requested function.

- If the panel is configured to require an Access Code and the code is not sent (or invalid) the panel will fail the function (unsuccessful).

- If the panel fails the function, an SMS response message is sent to the user. The SMS response will echo the command sent, followed by the label "unsuccessful". (e.g., "night arm partition 2 1234 unsuccessful").

- The partition label or partition number may be excluded from the SMS request in a single partition system (e.g., disarm 9123).

NOTE: The Cellular phone number can be viewed in Section [996] or by User entering *6 [<] [>] "Cellular Phone No." at the keypad. An Access Code is required for all SMS commands, except Help.

[601] Stay Arm
Default (Stay Arm);
Send this command to the system to stay arm. It may be followed by a Partition Label or partition number and Access Code.

[602] Away Arm
Default (Away Arm);
Send this command to the system to away arm. It may be followed by a Partition Label or partition number and Access Code.

[603] Night Arm
Default (Night Arm);
Send this command to the system to night arm. It may be followed by a Partition Label or partition number and Access Code.

[604] Disarm
Default (Disarm);
Send this command to the system to disarm. It may be followed by a Partition Label or partition number and Access Code.

[605] - [608] Activate Command Output 1 - 4
Default (Activate Command Output n);
Where n is a number from 1 - 4. Send this command to the system to activate a command output. It may be followed by a Partition Label or partition number and Access Code.

[609] - [612] Deactivate Command Output 1 - 4
Default (Deactivate Command Output n);
Where n is a number from 1 - 4. Send this command to the system to deactivate a command output . This command may be followed by a Partition Label or partition number and optional Access Code.

[613] Bypass
 Default (Bypass);
Send this command to the system to bypass a Zone. This command should be followed by a Zone label or Zone number and Access Code.

[614] Unbypass
Default (Unbypass);
Send this command to the system to unbypass a Zone. This command should be followed by the Zone label or Zone number and Access Code.

[615] Status Request
Default (Status Request);
Send this command to request the status of the system. It may be followed by a partition label or partition number and Access Code. If partition label is omitted, status of all enabled partitions will be sent. If there is a trouble on the system, the system label is sent, followed by the trouble label, then the partition status.

NOTE: Status Request response may require more than 1 SMS message, depending on status of the system. There is a 10 second delay between transmission of SMS messages.

[616] Alarm Memory Request
Default (Alarm Memory Request);
Send this command to the system to request the alarm memory from the system. This command may be followed by a Partition Label or partition number, and Access Code. If partition label is omitted, alarm memory of all partitions will be sent. Alarm memory responses will include Partition label and Zone label. Up to 8 partitions may be contained in 1 message.

NOTE: Alarm Memory Request response may require more than 1 SMS message, depending on alarm memory of the unit. There is a 10 second delay between transmission of SMS messages.

[617] Help
Default (Help);
When help is sent, the SMS response is a listing of all Interactive commands that can be sent to the module. Access Code is not required.

[619] Keypad Message
Default (Keypad Message);
The response format is: [Account Label] [Date and Time] [SMS Function] [Response] [Message Text]. Fields are space delimited.When Keypad Message is sent, the SMS response is the message displayed on the keypad. If the message is too long to display on the keypad, only the portion displayed is sent in the response.

SMS COMMAND AND CONTROL RESPONSE

NOTE: SMS Command and Control Response messages are up to 32 ASCII characters (Maximum 160 characters per SMS message). The message language is specified in Section [009]. SMS responses are sent to the phone that initiated the command.

[621] Function Successful
Default (Successful);
When an SMS Command and Control function is successfully performed by the panel, the successful label is included in the response sent to the user, following the command requested. (e.g., if "stay armed" command is completed by the panel, SMS response is: "stay armed successful").

[622] Function Unsuccessful
Default (Unsuccessful);
When an SMS Command and Control function is not successfully performed by the panel, the command sent to the unit will be included in the response sent to the user, followed by this label. (e.g., if "stay armed" command is not completed, SMS response is: "stay armed unsuccessful").

[623] Invalid Command
Default (Invalid Command);
This label will be included in the response message if the command was not accepted as a valid SMS command.

[624] System Stay Armed
Default (Stay Armed);
This label will be included in the response to a status request command if a partition is stay armed.

[625] System Away Armed
Default (Away Armed);
This label will be included in the response to a status request command if a partition is away armed.

[626] System Night Armed
Default (Night Armed);
This label will be included in the response to a status request command if a partition is night armed.

[627] System Disarmed Ready
Default (Disarmed Ready);
This label will be included in the response to a status request command if a partition is disarmed and is ready to arm.

[628] System Disarmed Not Ready
Default (Disarmed Not Ready);
This label will be included in the response to a status request command if a partition is disarmed and is not ready to arm.

[629] System is in Alarm
Default (is in Alarm);
This label will be included in the response to a status request command if a partition is in alarm.

[630] Trouble Label
Default (Service is Required);
This label will be included in the response to the Alarm Memory command if there are no alarms in memory.

[631] No Alarms in Memory
Default (No Alarm Memory);
This label will be included in the response to an Alarm Memory Request if there are no alarms on the system.

[634] Error Code
Default (Error Code);
When an SMS initiated function fails, the module will send an error code to the telephone number that was source of the SMS request. Message format is:[**Account Label] [Date and Time] [Error Code] [Error Type]**. Fields are "space" delimited. .

Table 15: Error Code Format

Class	Definition	Error	Definition
01	DLS	01	Bad SMS format
		02	Session failed due to local network issues
		03	Unable to connect to remote server
		04	Bad DLS access code
		05	DLS lockout active
02	TFTP	01	Bad SMS format
		02	Session failed due to local network issues
		03	Unable to connect to remote server
		04	File not found on TFTP server

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 [988] - [998] are provided for information (Read Only). Values can not be modified using these Sections.

[987] Language Version

This Section will display the current Language version of the Communicator. Currently this value is: 01.00.01.TT.

[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. Currently this value is: 01.20.01.TT.

[991] Firmware Version

This Section will display the current firmware version of the device. Currently this value is 01.20.01.TT.

[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 using [*] [6] [<] [>] "Cellular Phone No." to display the phone number used for SMS Command and Control functions.

[997] IMEI Number

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

[998] MAC Address

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

SYSTEM RESET DEFAULTS

[999] Software Default

Default (99)

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

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

11: **Default Labels**. All labels used for SMS Command and Control are reset to the default language programmed in Section [009].

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

66: Reactivate Module. The Communicator is reactivated. Upon reactivation, the first command received by the Communicator must be an INIT command.

NOTE: The Communicator is not reactivated by performing a Power Cycle.

ETHERNET/Cellular Programming Worksheets

SYSTEM OPTIONS

[001] Ethernet IP Address

Default (000.000.000.000); (TL255-SM/TL2553G-SM only)

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

[002] Ethernet IP Subnet Mask

Default (255.255.255.000); (TL255-SM/TL2553G-SM only)

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

[003] Ethernet Gateway IP Address

Default (000.000.000.000); (TL255-SM/TL2553G-SM only)

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

[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] TL260GS; [ON]GS2060.

|___| [5] Redundant Communications Default (OFF).

|___| [6] Remote Firmware Upgrade Default (ON).

|___| [7] Alternate Test Transmission Default (OFF).

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.

|___|___|___|___|

[020] Time Zone

Default (00) Valid range: 00 - FF.

|___|___|

[021] Account Code

Default (FFFFFF);

Valid range: 000001 - FFFFFE.

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

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.

|___|___|

[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).

[007] DNS Server IP 1

❶Programming not permitted on UL/ULC listed system.
   Default (000.000.000.000); (TL255-SM/TL2553G-SM only)

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

[008] DNS Server IP 2

❶Programming not permitted on UL/ULC listed system.
   Default (000.000.000.000); (TL255-SM/TL2553G-SM only)

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

[009] Language

Default (01);

Program label language 01 -29. Valid range: See Table 12

|___|___|

[010] System Toggle Options 3

|___| [1] 2 Way Audio over Cellular. Default (OFF).|

[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.

|___|___|

[030] FTC Restore

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

|___|___|

[031] Panel Tamper Alarm

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

|___|___|

[032] Panel Tamper Alarm Restore

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

|___|___|

ETHERNET RECEIVER 1 OPTIONS

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

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

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

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

[103] Ethernet Receiver 1 Address
Default (127.000.000.001);

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

ETHERNET RECEIVER 2 OPTIONS

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

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

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

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

ETHERNET OPTIONS

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

|___|___|___|___|

CELLULAR RECEIVER 1 OPTIONS

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

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

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

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

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

CELLULAR RECEIVER 2 OPTIONS

[211] Cellular Receiver 2 Account Code
Default (0000000000);
Valid range: 0000000001 - FFFFFFFFFE.

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

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

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

[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.

❶Programming not permitted on UL/ULC listed system.

———————————————————————————

[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 ( );

❶Programming not permitted on UL/ULC listed system.

———————————————————————————

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

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

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

[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 ( );
❶Programming not permitted on UL/ULC listed system.
32 Character ASCII characters.

———————————————————————————

[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.

|___|___|___|___|

DRAFT-02_by_MM

[215] Cellular Receiver 2 APN

Default ( );

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.

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

EVENT NOTIFICATION AND INTERACTIVE OPTIONS

GS2060/TL260GS only

[301] Command and Control Toggle Options

|____| [3] SMS Command and Control Default (OFF).

|____| [3] Interactive Default (ON).

|____| [5] SMS Character Format Default (OFF).

|____| [6] Long SMS Message Handling Default (OFF).

[311] SMS Telephone Number 1

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[312] SMS Telephone Number 2

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[313] SMS Telephone Number 3

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

AREA LABEL PROGRAMMING

GS2060/TL260GS only

[321] SMS Telephone Number 1 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[216] Cellular Receiver 2 Domain Name

Default ( );

❶Programming not permitted on UL/ULC listed system.

32 ASCII characters.

_____

[226] Cellular Trouble Delay

Default (00);

Program 00 disable or FF enable.

|____|____|

[227] Voice Call Timeout

Default (00);

Program 00 disable or FF enable.

|____|____|

[228] Voice Call Back Time

Default (0A);

Program 00 disable or FF enable.

|____|____|

[229] Voice Call Back Number

Default (SIM Telephone Number);

32 character ASCII.

_____

[314] SMS Telephone Number 4

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[315] SMS Telephone Number 5

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[316] SMS Telephone Number 6

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[317] SMS Telephone Number 7

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[318] SMS Telephone Number 8

Default ( );

4 - 32 digit telephone number. Blank is disabled.

_____

[322] SMS Telephone Number 2 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[323] SMS Telephone Number 3 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[324] SMS Telephone Number 4 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[325] SMS Telephone Number 5 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[326] SMS Telephone Number 6 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

AREA LABEL PROGRAMMING

[351] Account Label

Default (Security System);

_____

[352] System Label

Default (System Area);.

_____

[353] Partition 1 Label

Default [Partition 1].

_____

[354] Partition 2 Label

Default [Partition 2].

_____

[355] Partition 3 Label

Default [Partition 3].

_____

USER LABEL PROGRAMMING

Programming is 16 character ASCII text

[361] User 1 Label

Default [User 1].

_____

[362] User 2 Label

Default [User 2].

_____

[363] User 3 Label

Default [User 3].

_____

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[327] SMS Telephone Number 7 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[328] SMS Telephone Number 8 Toggle Options

|____| [1] SMS Notification Alarm/Restore Default (ON).

|____| [2] SMS Notification Tamper/Restore Default (ON).

|____| [3] SMS Notification Opening/Closing Default (ON).

|____| [4] SMS Notification System Maintenance Default (ON).

|____| [5] SMS Notification System Test Default (ON)

|____| [6] SMSNotification Communicator Events Default(ON).

|____| [7] SMS Notification Enabled Default (ON).

|____| [8] SMS Command and Control Enabled Default (ON).

[356] Partition 4 Label

Default [Partition 4].

_____

[357] Partition 5 Label

Default [Partition 5].

_____

[358] Partition 6 Label

Default [Partition 6].

_____

[359] Partition 7 Label

Default [Partition 7].

_____

[360] Partition 8 Label

Default [Partition 8].

_____

[364] User 4 Label

Default [User 4].

_____

[365] User 5 Label

Default [User 5].

_____

[366] User 6 Label

Default [User 6].

_____

[367] User 7 Label
    Default [User 7].
_____

[368] User 8 Label
    Default [User 8].
_____

[369] User 9 Label
    Default [User 9].
_____

[370] User 10 Label
    Default [User 10].
_____

[371] User 11 Label
    Default [User 11].
_____

[372] User 12 Label
    Default [User 12].
_____

[373] User 13 Label
    Default [User 13].
_____

[374] User 14 Label
    Default [User 14.]
_____

[375] User 15 Label
    Default [User 15].
_____

[376] User 16 Label
    Default [User 16].
_____

[377] User 17 Label
    Default [User 17].
_____

[378] User 18 Label
    Default [User 18].
_____

[379] User 19 Label
    Default [User 19].
_____

[380] User 20 Label
    Default [User 20].
_____

[381] User 21 Label
    Default [User 21].
_____

[382] User 22 Label
    Default [User 22].
_____

[383] User 23 Label
    Default [User 23].
_____

[384] User 24 Label
    Default [User 24].
_____

[385] User 25 Label
    Default [User 25].
_____

[386] User 26 Label
    Default [User 26].
_____

[387] User 27 Label
    Default [User 27].
_____

[388] User 28 Label
    Default [User 28].
_____

[389] User 29 Label
    Default [User 29].
_____

[390] User 30 Label
    Default [User 30].
_____

[391] User 31 Label
    Default [User 31].
_____

[392] User 32 Label
    Default [User 32].
_____

[393] User 33 Label
    Default [User 33].
_____

[394] User 34 Label
    Default [User 34].
_____

[395] User 35 Label
    Default [User 35].
_____

[396] User 36 Label
    Default [User 36].
_____

[397] User 37 Label
    Default [User 37].
_____

[398] User 38 Label
    Default [User 38].
_____

[399] User 39 Label
    Default [User 39].
_____

[400] User 40 Label
    Default [User 40].
_____

ZONE LABEL PROGRAMMING

[401] Zone 1 Label
    Default [Zone 1].
_____

[402] Zone 2 Label
    Default [Zone 2].
_____

[403] Zone 3 Label
Default [Zone 3].

_____

[404] Zone 4 Label
Default [Zone 4].

_____

[405] Zone 5 Label
Default [Zone 5].

_____

[406] Zone 6 Label
Default [Zone 6].

_____

[407] Zone 7 Label
Default [Zone 7].

_____

[408] Zone 8 Label
Default [Zone 8].

_____

[409] Zone 9 Label
Default [Zone 9].

_____

[410] Zone 10 Label
Default [Zone 10].

_____

[411] Zone 11 Label
Default [Zone 11].

_____

[412] Zone 12 Label
Default [Zone 12].

_____

[413] Zone 13 Label
Default [Zone 13].

_____

[414] Zone 14 Label
Default [Zone 14].

_____

[415] Zone 15 Label
Default [Zone 15].

_____

[416] Zone 16 Label
Default [Zone 16].

_____

[417] Zone 17 Label
Default [Zone 17].

_____

[418] Zone 18 Label
Default [Zone 18].

_____

[419] Zone 19 Label
Default [Zone 19].

_____

[420] Zone 20 Label
Default [Zone 20].

_____

[421] Zone 21 Label
Default [Zone 21].

_____

[422] Zone 22 Label
Default [Zone 22].

_____

[423] Zone 23 Label
Default [Zone 23].

_____

[424] Zone 24 Label
Default [Zone 24].

_____

[425] Zone 25 Label
Default [Zone 25].

_____

[426] Zone 26 Label
Default [Zone 26].

_____

[427] Zone 27 Label
Default [Zone 27].

_____

[428] Zone 28 Label
Default [Zone 28].

_____

[429] Zone 29 Label
Default [Zone 29].

_____

[430] Zone 30 Label
Default [Zone 30].

_____

[431] Zone 31 Label
Default [Zone 31].

_____

[432] Zone 32 Label
Default [Zone 32].

_____

[433] Zone 33 Label
Default [Zone 33].

_____

[434] Zone 34 Label
Default [Zone 34].

_____

[435] Zone 35 Label
Default [Zone 35].

_____

[436] Zone 36 Label
Default [Zone 36].

_____

[437] Zone 37 Label
Default [Zone 37].

_____

[438] Zone 38 Label
Default [Zone 38].

_____

[439] Zone 39 Label
Default [Zone 39].

_____

[440] Zone 40 Label
Default [Zone 40].

_____

[441] Zone 41 Label
> Default [Zone 41].

_____

[442] Zone 42 Label
> Default [Zone 42].

_____

[443] Zone 43 Label
> Default [Zone 43].

_____

[444] Zone 44 Label
> Default [Zone 44].

_____

[445] Zone 45 Label
> Default [Zone 45] .

_____

[446] Zone 46 Label
> Default [Zone 46].

_____

[447] Zone 47 Label
> Default [Zone 47].

_____

[448] Zone 48 Label
> Default [Zone 48].

_____

[449] Zone 49 Label
> Default [Zone 49]

_____

[450] Zone 50 Label
> Default [Zone 50].

_____

[451] Zone 51 Label
> Default [Zone 51].

_____

[452] Zone 52 Label
> Default [Zone 52].

_____

[453] Zone 53 Label
> Default [Zone 53].

_____

[454] Zone 54 Label
> Default [Zone 54].

_____

[455] Zone 55 Label
> Default [Zone 55].

_____

[456] Zone 56 Label
> Default [Zone 56] .

_____

[457] Zone 57 Label
> Default [Zone 57].

_____

[458] Zone 58 Label
> Default [Zone 58].

_____

[459] Zone 59 Label
> Default [Zone 59].

_____

[460] Zone 60 Label
> Default [Zone 60].

_____

[461] Zone 61 Label
> Default [Zone 61].

_____

[462] Zone 62 Label
> Default [Zone 62].

_____

[463] Zone 63 Label
> Default [Zone 63].

_____

[464] Zone 64 Label
> Default [Zone 64].

_____

PANEL EVENT LABEL PROGRAMMING

[501] Burglary Alarm
> Default [Burglary Alarm].

_____

[502] Burglary Alarm Restore
> Default [Burglary Alarm Restore].

_____

[503] Fire Alarm
> Default [Fire Alarm].

_____

[504] Fire Alarm Restore
> Default [Fire Alarm Restore].

_____

[505] 24 Hour Alarm
> Default [24 Hour Alarm].

_____

[506] 24 Hour Alarm Restore
> Default [24 Hour Alarm Restore].

_____

[507] Holdup Alarm
> Default [Holdup Alarm].

_____

[508] Holdup Alarm Restore
> Default [Holdup Alarm Restore].

_____

[509] Gas Alarm
> Default [Gas / Carbon Monoxide Alarm].

_____

[510] Gas Alarm Restore
> Default [Gas / Carbon Monoxide Restore].

_____

[511] Heat Alarm
> Default [High Temperature Alarm].

_____

[512] Heat Alarm Restore
> Default [High Temperature Alarm Restore].

_____

[513] Medical Alarm
    Default [Medical Alarm].

_____

[514] Medical Alarm Restore
    Default [Medical Alarm Restore].

_____

[515] Panic Alarm
    Default [Panic Alarm].

_____

[516] Panic Alarm Restore
    Default [Panic Alarm Restore].

_____

[517] Emergency Alarm
    Default [Emergency Alarm].

_____

[518] Emergency Alarm Restore
    Default [Emergency Alarm Restore].

_____

[519] Sprinkler Alarm
    Default [Sprinkler Alarm].

_____

[520] Sprinkler Alarm Restore
    Default [Sprinkler Alarm Restore].

_____

[521] Water Level Alarm
    Default [Water Level Alarm].

_____

[522] Water Level Alarm Restore
    Default [Water Level Alarm Restore].

_____

[523] Freeze Alarm
    Default [Low Temperature Alarm].

_____

[524] Freeze Alarm Restore
    Default [Low Temperature Alarm Restore].

_____

[525] Fire Supervisory
    Default [Fire Supervisory].

_____

[526] Fire Supervisory Restore
    Default [Fire Supervisory Restore].

_____

[527] Zone Tamper
    Default [Zone Tamper].

_____

[528] Zone Tamper Restore
    Default [Zone Tamper Restore].

_____

[529] Zone Fault
    Default [Zone Fault].

_____

[530] Zone Fault Restore
    Default [Zone Fault Restore].

_____

[531] Fire Trouble
    Default [Fire Trouble].

_____

[532] Fire Trouble Restore
    Default [Fire Trouble Restore].

_____

[533] Module Supervisory
    Default [Module Supervisory Trouble].

_____

[534] Module Supervisory Restore
    Default [Module Supervisory Restore].

_____

[535] General System Tamper
    Default [General System Tamper].

_____

[536] General System Tamper Restore
    Default [General System Tamper Restore].

_____

[537] Wireless Device Low Battery
    Default [Wireless Device Low Battery].

_____

[538] Wireless Device Low Battery Restore
    Default [Wireless Device Battery Restore].

_____

[539] Cross Zone/Police Code
    Default [Burglary Verified].

_____

[540] Burglary Not Verified
    Default [Burglary Not Verified].

_____

[541] Duress Alarm
    Default [Duress Alarm].

_____

[542] Opening After Alarm
    Default [Disarmed After Alarm].

_____

[543] Recent Closing
    Default [Alarm Occurred After Arming].

_____

[544] Alarm Canceled
    Default [Alarm Canceled].

_____

[545] Keypad Lockout
    Default [Keypad Lockout].

_____

[546] Exit Fault
    Default [Exit Fault].

_____

[547] Partial Closing
    Default [Armed With Zones Bypassed].

_____

[548] Zone Bypass
    Default [Zone Bypassed].

_____

[549] Zone Unbypass

    Default [Zone Unbypassed].

_____

[550] Auto Arm Cancel

    Default [Automatic Arming Cancelled].

_____

[551] Closing

    Default [Armed By].

_____

[552] Opening Label

    Default [Disarmed By].

_____

[553] Special Closing

    Default [Armed].

_____

[554] Special Opening

    Default [Disarmed].

_____

[555] Late to Open

    Default [Late to Open].

_____

[556] Delinquency

    Default [Delinquency].

_____

[557] General System Trouble

    Default [General System Trouble].

_____

[558] General System Trouble Restore

    Default [General System Trouble Restore].

_____

[559] AC Line Trouble

    Default [AC Power Failure].

_____

[560] AC Line Trouble Restore

    Default [AC Power Restore].

_____

[561] Battery Trouble

    Default [Battery Trouble].

_____

[562] Battery Trouble Restore

    Default [Battery Restore].

_____

[563] Bell Circuit Trouble

    Default [Bell Circuit Trouble].

_____

[564] Bell Circuit Trouble Restore

    Default [Bell Circuit Restore].

_____

COMMUNICATOR EVENT LABEL PROGRAMMING

[591] Panel Absent Trouble

    Default [Panel Communications Trouble].

_____

[592] Panel Absent Trouble Restore

    Default [Panel Communications Restored].

_____

[565] Auxiliary Power Trouble

    Default [Auxiliary Power Trouble].

_____

[566] Auxiliary Power Trouble Restore

    Default [Auxiliary Power Restore].

_____

[567] Ground Fault

    Default [Ground Fault Trouble].

_____

[568] Ground Fault Restore

    Default [Ground Fault Restore].

_____

[569] TLM Failure

    Default [Telephone Line Failure].

_____

[570] TLM Failure Restore

    Default [Telephone Line Restore].

_____

[571] FTC Trouble

    Default [Fail To Communicate Trouble].

_____

[572] FTC Restore

    Default [Fail To Communicate Restore].

_____

[573] Event Buffer 75% Full

    Default [Event Buffer Near Full].

_____

[574] DLS Lead In

    Default [Remote Programming Begin].

_____

[575] DLS Lead Out

    Default [Remote Programming End].

_____

[576] Installer Lead In

    Default [Local Programming Begin].

_____

[577] Installer Lead Out

    Default [Local Programming End].

_____

[578] Walk Test Lead In

    Default [Walk Test Begin].

_____

[579] Walk Test Lead Out

    Default [Walk Test End].

_____

[580] System Test

    Default [System Test Message].

_____

[593] Module Reprogramming

    Default [Communicator Programming Updated].

_____

[594] Firmware Update

    Default [Communicator Firmware Updated].

_____

SMS COMMAND AND CONTROL FUNCTIONS

[601] Stay Arm

Default (Stay Arm);

_____

[602] Away Arm

Default (Away Arm);

_____

[603] Night Arm

Default (Night Arm);

_____

[604] Disarm

Default (Disarm);

_____

[605] Activate Command Output 1

Default [Activate Command Output 1].

_____

[606] Activate Command Output 2

Default [Activate Command Output 2].

_____

[607] Activate Command Output 3

Default [Activate Command Output 3].

_____

[608] Activate Command Output 4

Default [Activate Command Output 4].

_____

[609] Deactivate Command Output 1

Default [Deactivate Command Output 1].

_____

[610] Deactivate Command Output 2

Default [deactivate command output 2].

_____

[611] Deactivate Command Output 3

Default [Deactivate Command Output 3].

_____

[612] Deactivate Command Output 4

Default [Deactivate Command Output 4].

_____

[613] Bypass

Default (Bypass);

_____

[614] Unbypass

Default (Unbypass);

_____

[615] Status Request

Default (Status Request);.

_____

[616] Alarm Memory Request

Default (Alarm Memory Request);

_____

[617] Help

Default (Help);

_____

[619] Keypad Message

Default (Keypad Message);

_____

SMS COMMAND AND CONTROL RESPONSE

[621] Function Successful

Default (Successful);

_____

[622] Function Unsuccessful

Default (Unsuccessful);

_____

[623] Invalid Command

Default (Invalid Command);

_____

[624] System Stay Armed

Default (Stay Armed);

_____

[625] System Away Armed

Default (Away Armed);

_____

[626] System Night Armed

Default (Night Armed);

_____

[627] System Disarmed Ready

Default (Disarmed Ready);

_____

[628] System Disarmed Not Ready

Default (Disarmed Not Ready);

_____

[629] System is in Alarm

Default (is in Alarm);

_____

[630] Trouble Label

Default (Service is Required);

_____

[631] No Alarms in Memory

Default (No Alarm Memory);

_____

[634] Error Code

Default (Error Code);

_____

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

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

SYSTEM RESET DEFAULTS

[999] Software Default
   Default (99) Valid entries are 00; 11; 55; 66.

|___|___|

[995] SIM Number

_____

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

_____

[997] IMEI Number

_____

[998] MAC Address

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

DRAFT-02_by_MM

END USER LICENCE AGREEMENT

IMPORTANT - READ CAREFULLY: DSC Software purchased with or without Products and Components is Copyrighted and is pur-chased 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 PROD-UCT, 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 SOFT-WARE 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 Class B digital apparatus complies with Canadian ICES-003.

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

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

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

DRAFT-02_by_MM

29007848R001

DSC
A Tyco International Company