

D9412GV3/D7412GV3 v8.03 to v8.05



EN | Program Entry Guide
Control Panels



BOSCH



System Requirements



Minimum system requirements for Classification in accordance with ANSI/SIA CP-01-2007:

- UL Listed and Classified control unit Model D9412GV3 or D7412GV3
- UL Listed and Classified keypad Model D1256, D1257, D1260, D1255, D1255R, or D1255 RW
- UL Listed Local Bell

The minimum firmware requirements for SIA CP-01 compliance are:

Control Panel	Firmware Version
D9412GV3	8.0 or later
D7412GV3	8.0 or later

Trademarks

CoBox is a registered trademark of Lantronix.

Windows is a registered trademark of Microsoft Corporation in the United States or in other countries.

Molex is a registered trademark of Molex Incorporated.

Documentation Conventions

Type Styles Used in this Manual

To help identify important items in the text, the following type styles are used:

Prompt

A thick border is used to indicate a main programming entry as seen in the Remote Programmer's Display. It is used as a section heading and screen example. Shaded boxes indicate programmer prompts that are only available when Custom or View events are selected.

Sub-Prompt

A dashed border indicates a sub entry under a main programming entry.

Warnings, Cautions, and Notes

Throughout this document helpful tips and notes are presented concerning the entire application or programming the unit. They are displayed as follows:



Warning!

These warn of the possibility of physical damage to the operator, program and/or equipment. Use this when there is an increased risk of physical damage to the operator (severe injury or death) or equipment (destruction of physical components).



Caution

These caution the operator that physical damage to the program and/or equipment.



Important Notes

These notes should be heeded for successful operation and programming.

Table of Contents

1.0	Introduction	4	2.10.1	Keypad (Command Center) Assignment.....	50
1.1	Using this Program Entry Guide.....	4	2.10.2	Area Text.....	56
1.2	Product Handlers	6	2.11	User Interface	60
1.3	Guide to Programming Options	7	2.11.1	Commands.....	60
1.4	Programming the Control Panel with the D5200 Programmer.....	7	2.11.2	Keypad Selections	60
1.5	Guide to UL 864 Programming Requirements 8		2.11.3	Access Control Functions	63
2.0	GV2MAIN.....	11	2.11.4	Authority Level Selections	67
2.1	Phone	11	2.11.5	Access Control Levels.....	75
2.2	Phone Parameters	12	2.11.6	SIA Duress Passcode Options.....	77
2.2.1	Special Point/User Reporting.....	14	2.12	Function List.....	77
2.3	Routing.....	16	2.13	Relay Parameters	78
2.3.1	Called Party Disconnect	16	2.13.1	Area Relays	79
2.3.2	Route Number Groups: Which Has the Highest Priority?	16	2.13.2	Panel-Wide Relays	81
2.3.3	Programming Primary and Backup Destinations.....	16	3.1	Passcode or Token Worksheet.....	82
2.3.4	Enhanced Routing	16	3.1.1	User Groups.....	83
2.3.5	Programming a Duplicate Report.....	16	3.1.2	Passcodes.....	83
2.3.6	Routing Destination Communication Failures	16	3.1.3	User Group Window	83
2.3.7	Message Prioritization within a Route Number	17	3.1.4	User Name	83
2.3.8	Dialing Attempts.....	17	3.1.5	Tokens and Cards.....	83
2.4	Enhanced Routing.....	24	3.1.6	Reporting and Logging	84
2.4.1	Programming a Primary and Backup Destination.....	24	4.0	RADXPNTS	87
2.4.2	Programming a Duplicate Report.....	24	4.1	Point Index	87
2.4.3	Numeric Pager Capability.....	26	4.2	Point Responses	91
2.5	Power Supervision.....	28	4.2.1	Applications for Point Responses 9, D, and E:	91
2.6	Printer Parameters	30	4.2.2	Characteristics of a Fire Point:.....	91
2.7	RPS Parameters.....	32	4.3	Point Assignments.....	101
2.7.1	Uploading and Downloading Reports	32	4.4	COMMAND 7 and COMMAND 9	103
2.7.2	Log Threshold Reports	33	5.0	RADXSKE.....	105
2.7.3	RPS Callback Reports	33	5.1	Windows	105
2.8	Miscellaneous	35	5.1.1	Opening and Closing	105
2.9	Area Parameters.....	36	5.1.2	User Group Windows	112
2.9.1	Area Parameters.....	36	5.1.3	Holiday Indexes for User Group Windows	114
2.9.2	Programming Account Numbers in 9000 Series Control Panels	36	5.2	Skeds	114
2.9.3	Shared-Area Characteristics.....	41	5.3	Holiday Indexes.....	123
2.9.4	Bell Parameters	41	5.3.1	Add/Change/Delete	123
2.9.5	Open/Close Options.....	43	5.3.2	View Holidays	124
2.9.6	Arming Features	47	6.0	GV2AUX.....	124
2.10	Keypad (Command Center)	50	6.1	Introduction	124
			6.2	RPS and D5200 Handler Requirements....	124
			6.3	SDI Automation	125
			6.4	SDI RPS Parameters.....	126
			6.4.1	User Interface Modifications for COMMAND 43.....	127
			6.4.2	Using an External Modem	129
			6.5	Programming Path Numbers and IP Addresses for Enhanced Communications	134

6.6	SDI RPS/Enhanced Communications Configuration	138
6.7	Route Group Rates	139
6.8	Miscellaneous.....	139
6.9	Cross Point Parameters	142
7.0	RADXAXS	144
7.1	Door Profile.....	144
7.2	Strike Profile	147
7.3	Event Profile	148
8.0	SIA CP-01 Quick Reference	150
	Programming Prompts Directory	151

Figures

Figure 1:	Pager Display Fields.....	26
Figure 2:	Account Number Entry	37
Figure 3:	Softkey Locations on the D1260 Keypad	58
Figure 4:	User Group 122 Example	84
Figure 5:	Example Opening Window Timeline (using two Opening Windows on same day) ..	107
Figure 6:	COMMAND 43 Flow Chart	128
Figure 7:	RPS IP Address Prompts	129
Figure 8:	Com Port Selection within HyperTerminal	130
Figure 9:	External Modem Connection	131
Figure 10:	Path # IP Add1 to Add4	134
Figure 11:	Poll Rate Timeline.....	136

Tables

Table 1:	Differences between the D9412GV3 and D7412GV3.....	5
Table 2:	Literature Referenced	5
Table 3:	Product Handlers.....	6
Table 4:	Programming Error Displays.....	7
Table 5:	UL 864 Programming Requirements.....	8
Table 6:	UL 864 Programming Recommendations	10
Table 7:	Modem IIIa ² Communication Format Data - User ID Numbers	13
Table 8:	Modem IIIa ² Communication Format Data - Point Numbers.....	13
Table 9:	D6000 User IDs and Zones	14
Table 10:	SDI Path Number by Device	16
Table 11:	Fire Reports.....	18
Table 12:	Burglar Reports.....	18
Table 13:	User Reports	18
Table 14:	Test Reports.....	20

Table 15:	Diagnostic Reports	20
Table 16:	Relay Reports.....	21
Table 17:	Auto-Function Reports	21
Table 18:	RPS Reports.....	22
Table 19:	Point Reports.....	22
Table 20:	User Change Reports.....	23
Table 21:	Access Reports	23
Table 22:	Event Descriptions, Priorities, and Numbers.....	27
Table 23:	Programming Four-Digit Account Numbers.....	36
Table 24:	Programming Ten Digit Account Numbers	37
Table 25:	Verify Time.....	39
Table 26:	CF### Key Strokes.....	58
Table 27:	CF### Custom Function Keystrokes	59
Table 28:	Keypad Programming Choices	60
Table 29:	Authority Level Selections	67
Table 30:	L## Secure Door-Door Mode Definitions	71
Table 31:	Bypassing a Point.....	98
Table 32:	P### BFSK/Relay Codes/Relays	102
Table 33:	Point Text for Points 240 to 247	103
Table 34:	Window Selections	105
Table 35:	Programming for Two Same Day Opening Windows (refer to <i>Figure 5</i>) ..	108
Table 36:	Programming to Link Two Days over Midnight*	108
Table 37:	Programming Example: Linking Two Closing Windows over Midnight.....	109
Table 38:	Opening and Closing Windows Worksheet.....	111
Table 39:	Opening and Closing Windows.....	111
Table 40:	Normal Store Hours*	111
Table 41:	Delivery Schedule*	112
Table 42:	Monthly Auditor's Schedule*	112
Table 43:	Cross Point Ranges Within Groups	143
Table 44:	Effects of Programming on Custom Function Activation	145
Table 45:	Programming the Control Panels for SIA CP--01 Compliance	150

1.0 Introduction

1.1 Using this Program Entry Guide

This guide is only for programming the D9412GV3 and D7412GV3 Control Panels.

Although this guide specifically refers to the D9412GV3 Control Panels, it can be used for programming the D7412GV3 Control Panels. Differences between the D9412GV3 and D7412GV3 are shown in *Table 1*.

Table 1: Differences between the D9412GV3 and D7412GV3

Features	D9412GV3	D7412GV3
Access Control	Eight Doors	Two Doors
Expanded users		
Passcodes	249	99
Cards/tokens	996	396
Passcode-protected custom functions	16	4
Number of printers	3	1
Number of points	246	75
Number of relays	128	64



Throughout this guide and in the control panel programming, where applicable, BFSK now refers to Contact ID.

Table 2: Literature Referenced

Document Name	Part Number
<i>D1255 Installation Instructions</i>	74-06819-000
<i>D1256/D1257 Installation Instructions</i>	74-06925-000
<i>D1255RBD1256RBD1257RB Installation Instructions</i>	F01U011791
<i>D1260 Installation Guide</i>	48101
<i>D1260 Owner's Manual</i>	50410
<i>D5200 Programmer Operation Manual</i>	74-06176-000
<i>D6500 Report Directory</i>	74-04651-001
<i>Conettix D6600/6100 Receiver/Gateway Program Entry Guide</i>	4998122702
<i>Conettix D6600/6100 Receiver/Gateway Computer Interface Manual</i>	4998122703
<i>D720 Series Installation Guide</i>	74-06918-000
<i>D9210B Operation and Installation Guide</i>	32206
<i>D9210B Program Entry Guide</i>	32207
<i>D9210B Program Record Sheet</i>	32208
<i>D9412GV3/D7412GV3 Operation and Installation Guide</i>	F01U143070
<i>D9412GV3/D7412GV3 Program Record Sheet</i>	F01U143072
<i>RPS Installation and Operation Guide</i>	4998141259

1.2 Product Handlers

Programming the GV3 requires multiple product handlers. The availability of each handler is indicated in *Table 3*. Refer to the specific control panel's release notes to determine the most current handler versions.

Although the handlers shown in *Table 3* can be used to program any of the new control panels, not all of the functions operate. For example, the RADXUSR1 Handler programs users 000 through 124. Even though the handler allows you to program users 100 through 124, the D7412GV3 does not allow the activation of these users.

Table 3: Product Handlers				
Product Handler	Compatible Versions	Function	D9412GV3	D7412GV3
GV2MAIN	V1.04 and above	Covers Panel-Wide, Area, Keypad Function List, User Interface, and Relay programming modules.	✓	✓
RADXUSR1	V1.06 and above	Covers passcode and token programming for users 000 through 124 (users 000 through 099 for the D7412GV3).	✓	✓
RADXUSR2	V1.05 and above	Covers passcode and token programming for Users 125 through 249.	✓	N/A
RADXPNTS	V1.08 and above	Covers Point Index and Point Assignment programming for all points.	✓	✓
RADXSKED	V1.04 and above	Covers Open/Close Windows, User Access Windows, Skeds, and Holiday Index programming modules.	✓	✓
GV2AUX	V1.04 and above	Covers SDI Automation, SDI RPS Parameters, Enhanced Communication Parameters, Route Group Attempts, Miscellaneous, and Cross Point Parameters.	✓	✓
RADXAXS	V1.06 and above	Covers the programming parameters for installed D9210B Door Controllers. The program entry guide and program record sheet for this handler come with the D9210B Access Control Module.	✓	✓

1.3 Guide to Programming Options

This guide is set up in a specific order. Related program entries are grouped together in modules as they appear in the specific product handlers. The handler and the programming module are listed at the top of each page to help you find specific programming prompts.

This guide shows the programming options for each product handler. Each option is listed with:

- **The Program Item Prompt:** Each prompt is shown as it appears in the D5200 Programmer [refer to the *D5200 Programmer Operation Manual* (P/N: 74-06176-000)] or the Remote Programming Software (RPS). Refer to the *RPS Installation and Operation Guide* (P/N: 4998141259). For space considerations, some prompts must be abbreviated in the Programmer display. In these cases, the meaning of the prompt is explained below the prompt
- **Program Entry Default Setting:** Because defaults are set for the typical installation, programming each prompt might not be necessary. Review the default entries in the program record sheet shipped with the control panel to determine which prompts must be programmed.
- **Program Entry Selections:** Only the selections listed can be used for a particular program item.
- **Program Entry Description:** Describes the various entry selections. Read the descriptions carefully to avoid improperly programmed equipment.
- **Custom Programming:** Select custom programming (**Yes** or **No**) to expand programming modules within the D5200. Programming Custom as **Yes** allows parameters for special applications to be visible in the programmer.

1.4 Programming the Control Panel with the D5200 Programmer



Caution: Do not connect the D5200 to the PROG connector without closing the reset switch. Doing so causes SDI ## TROUBLE and CALL FOR SERVICE to display on the keypads. Door controllers also activate, depending upon the SDI failure DIP switch setting.



To acquire an update for your D5200 Programmer, call the Bosch Security Systems, Inc. Handler Update System at (800) 657-4584. Make a separate phone call for each handler.

Use an analog telephone line with the D5200. The D5200 dials only pulses.

Refer to *Section 10 Updating Handlers* in the *D5200 Programmer Operation Manual* (P/N: 74-06176-000) for details on updating handlers.

- To connect the D5200 Programmer to the control panel:
 1. Close the reset switch, located in the upper right corner of the control panel and labeled S1 Reset, to place the D9412GV3 or D7412GV3 Control Panel in the standby mode.
 2. Connect the Molex connector at one end of the cord to the connector labeled PROG on the PCB and PROG CONN on the faceplate.
- To retrieve the current control panel configuration, press the [RECV (COPY)] key on the D5200 at the NEWRECORD prompt. Refer to the *D5200 Programmer Operation Manual* (P/N: 74-06176-000) for detailed information.
- To write new configuration information for the control panel, press the [SEND (LOAD)] key at the NEWRECORD prompt. Refer to the *D5200 Programmer Operation Manual* (P/N: 74-06176-000) for detailed information.
- To disconnect the D5200:
 1. Disconnect the Molex connector.
 2. Open the reset switch.



When the reset switch is opened, the control panel reboots and resumes normal operation within 5 to 25 sec.

Table 4: Programming Error Displays

Display	Description
INCOMPATIBLE PANEL	You are connected to the wrong control panel or using the wrong handler. Check the faceplate for the model number and the handler title.
CHECK CORD/RESET PIN	Check the cord and the reset pin

1.5 Guide to UL 864 Programming Requirements

This section identifies the programming requirements you must make in order to comply with UL 864 Commercial Fire applications.



NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES

This product incorporates field-programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, you must limit certain programming features or options to specific values. Refer to *Table 5*.

Table 5: UL 864 Programming Requirements

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864	Refer to Page:
If using two phone lines:				
Phone 1 through 4	Yes	24 characters	Program a valid phone number	11 to 12
Phone Supervision	Yes	0 to 240 sec	10 to 200 sec	14
Alarm On Fail	No	Yes / No	Set to No	14
Buzz On Fail	Yes	Yes / No	Set to Yes	15
Two Phone Lines	Yes	Yes / No	Set to Yes when using PSTN communications.	15
Expand Test Report	Yes	Yes/No	Set to Yes	15
Fire Reports	Yes	Yes / No	Set to Yes	18
R# Fire Supervisory Missing	Required	Yes/No	Set to Yes	18 (<i>Table 11</i>)
Test Reports	Yes	Yes / No	Set to Yes	19
AC Fail Report	Yes	Yes / No	Set to Yes	20 (<i>Table 15</i>)
AC Restoral Report	Yes	Yes / No	Set to Yes	20 (<i>Table 15</i>)
Battery Missing Report	Yes	Yes / No	Set to Yes	20 (<i>Table 15</i>)
Low Battery Report	Yes	Yes / No	Set to Yes	20 (<i>Table 15</i>)
Battery Restoral Report	Yes	Yes / No	Set to Yes	20 (<i>Table 15</i>)
RG#1 Primary SDI (88)	Yes	Yes / No	Set to Yes	24
RG#1 Backup SDI (88)	Yes	Yes / No	Set to Yes	24
RG#1 Primary SDI (92)	Yes	Yes / No	Set to Yes	24
RG#1 Backup SDI (92)	Yes	Yes / No	Set to Yes	24
R# Service Start Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
R# Service End Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
R# Fire Walk St Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
R# Fire Walk End Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
R# Walk Test St Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
R# Walk Test End Report	Required	Yes / No	Set to Yes	22 (<i>Table 19</i>)
RG #1 Primary Device	N/A	1 to 4	Must have 1 to 4	24
RG #1 Backup Device	N/A	1 to 4	Must have 1 to 4	24
AC Fail Time	Yes	1 to 90	Enter 61	28
AC Fail Display	Yes	10 to 300 sec	10 to 200 sec	29
AC Tag Along	Yes	Yes / No	Set to Yes	30
AC/Battery Buzz	Yes	Yes / No	Set to Yes	30

Table 5: UL 864 Programming Requirements (continued)

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864	Refer to Page:
Bat Fail/Res Rpt	Yes	Yes / No	Set to Yes	30
Area 1 Area On	Required to send system status reports	Yes / No	Set to Yes	36
A# Delay Res	Yes	Yes / No	Set to Yes	37
Verify Time	Yes	10 to 60 sec	60 sec	38
Area # Fire Time	Yes	1 to 90 min	5 min (check with AHJ)	42
CC# Supervised	Yes	Yes / No	Set to Yes	51
CC# Trouble Tone	Yes	Yes / No	Set to Yes	53
CC# Scroll Lock	Yes	Yes / No	Set to Yes	55
Remote Program	Disable / Enable	Blank, E, or P	Set to P	65
A# Fire Bell	Yes	A,B,C, 1 to 128, Blank	Program with a relay	79
A# Reset Sensors	Yes	A,B,C, 1 to 128, Blank	Program with a relay	79
U### Area # Auth	Yes	1 to 8, Blank	Program an Authority Level for the Fire Area	84
U### Passcode	Yes	3-, 4-, 5-, or 6-digit passcode	Must program at least one passcode	85
P## Silent Bell	No	Yes / No	Set to No	93
P## Invisible Pt	No	Yes / No	Set to No	94
P## Local While Disarmed	No	Yes / No	Set to No	96
P## Local While Armed	No	Yes / No	Set to No	97
P## Disable Rst	No	Yes / No	Set to No	97
P## Bypassable	No	Yes / No	Set to No	98
P## Swinger Byps	No	Yes / No	Set to No	99
P## Fire Point	Yes	Yes / No	Set to Yes	100
P## Resettable	Yes	Yes / No	As required	100
Sked## Function Code	Required	1 to 11, 13 to 28	Sked Function Code 9	114
Sked## Defer Test	No	Yes / No	Set to No	117
Sked## Hourly Test (Report?)	No	Yes / No	Set to No	117
Sked## Time	Enter valid time	00:00 to 23:59	00:00 to 23:59	122
Sked## Date	No	mm/dd	Set to No	122
Sked## Sunday	Yes	Yes / No	Set to Yes	122
Sked## Monday	Yes	Yes / No	Set to Yes	122
Sked## Tuesday	Yes	Yes / No	Set to Yes	122
Sked## Wednesday	Yes	Yes / No	Set to Yes	122
Sked## Thursday	Yes	Yes / No	Set to Yes	122
Sked## Friday	Yes	Yes / No	Set to Yes	122
Sked## Saturday	Yes	Yes / No	Set to Yes	122
Sked## Xept On Holiday	No	Yes / No	Set to No	123

Table 5: UL 864 Programming Requirements (continued)

Product Feature/Option	Permitted in	Possible Settings	Settings Permitted in	Refer to
------------------------	--------------	-------------------	-----------------------	----------

	UL 864? (Y/N)		UL 864	Page:
For IP Communications to a D6600 Receiver				
Enhanced Comm	Yes	Yes / No	Set to Yes	134
Path1 IP Add1 (2, 3 or 4)	Yes	000 to 255	Program a valid IP address	134 – 135
Path 1 Poll Rate	Yes	0, 5 to 65535 sec*	Program as necessary	135
Path 1 Ack Wait	Yes	0, 5 to 65535 sec*	Program as necessary	137
Path 1 Retry Count	Yes	0 to 255	Program as necessary	137
9133 Supervision	Yes	Yes / No	Set to Yes	139
For Ground Fault Enable Switch				
(Refer to the D9412GV3/D7412GV3 Operation and Installation Guide (P/N: F01U143070))	Yes	Closed = Enabled Open = Disabled	Closed	N/A
* Set the Path 1 Poll Rate to 65535 for 24 hr.				

The following programmable parameters are recommended by Bosch when installing a commercial fire alarm system. Always check with your local Authority Having Jurisdiction.

Table 6: UL 864 Programming Recommendations

Prompt	Possible Settings	Recommendation
Phone Line Fail Report	Yes / No	Yes
Phone Line Restoral Report	Yes / No	Yes
Fire Walk Start Report	Yes / No	Yes
Fire Walk End Report	Yes / No	Yes
Cancel Report	Yes / No	Yes
CC# Scope	Panel Wide, Account Wide, Area Wide, Custom, No Keypad	Do not program No Keypad
CC# EnhancCmdCtr	Yes / No	Set to Yes , if applicable
CC# Menu Key Lock	Yes / No	If using D1256RB, set to No
Reset Sensors	Disable/Enable/Passcode Protect	Enable
Fire Test	Disable / Enable / Passcode Protect	Enable
L## Reset Sensors	Disable / Enable	If Reset Sensor is set to Passcode Protect , set this to Enable
L## Fire Test	Disable / Enable	If Fire Test is set to Passcode Protect , set this to Enable
U### User Group	Blank, 1 to 8	Program as blank
P## Ring Til Rst	Yes / No	May be required for Waterflow , otherwise No
P## Cross Point	Yes / No	Set to No for Fire devices.
D# Fire Unlock	Yes / No	No

2.0 GV2MAIN

Use GV2MAIN programming module to define the operating characteristics that affect panel-wide functions. This module has nine programming categories:

- Phone
- Phone Parameters
- Routing
- Enhanced Communications
- Area Parameters
- Keypad
- User Interface
- Function List
- Relay Parameters.

2.1 Phone

The control panel can dial as many as four different telephone numbers when sending event reports. All telephone numbers use the same receiver format. Refer to *Section 2.3 Routing* on page 16 for information about event report routing and communication protocols.



When using PSTN telephone lines, program two telephone numbers to meet UL 864 requirements.

Phone 1

Default:	Blank
Selection:	Up to 24 characters (do not enter [SPACE])
0 to 9	Numbers 0 through 9
C	3-sec pause
D	7-sec dial-tone detection
# or *	Used for the same purpose as pressing this key on a telephone keypad when manually dialing. For example, an asterisk (*) may be needed to access your long distance service. Do not use these characters when pulse dialing.
Blank	Control panel dials no phone number. Programming this item Blank does not disable phone routing. To disable reporting to this phone, refer to <i>Section 2.3 Routing</i> on page 16.

This is the telephone number the control panel dials to contact the central station receiver when sending event reports. This number is Phone 1 referred to in the prompts in *Section 2.3 Routing* on page 16.

The control panel waits for a break in the dial tone after dialing the first digit. If the control panel must dial a digit (for example, 9) to access an outside line, place a C before the phone number. The control panel waits 2 sec and does not wait for the dial tone break.

The control panel is programmed with a 7-sec dial tone detect period. When a dial tone is detected or the waiting period ends, the control panel begins to dial. To extend the dial tone detect period, place a D before the phone number. To insert a pause during or after dialing, use C in the number sequence. For example, if the control panel hangs up before it hears the Modem IIIa² ACK tone from the D6500 or D6600, program extra Cs after the phone number. The control panel waits on line for two extra seconds for each C programmed.

Enter up to 24 of the characters shown in the **Phone 1** table to define dialing characteristics.



Using both phone-data entry lines: The first line of the phone number data entry line must be filled (twelve characters) before you press [ENTER] to move to the second line. If you enter characters on the second line, and the first line has less than twelve characters, the second line clears when you press [ENTER].

For SIA CP-01 Compliance

Call Waiting Disable

If the telephone system at the installation site uses the Call Waiting feature, ensure that the backup telephone reporting number is programmed to disable Call Waiting.

If you program the primary phone number with a sequence to temporarily disable Call Waiting (typically *70 pause, but verify with the phone service provider) followed by the phone number, you should program the backup phone number without the Call Waiting cancel sequence. If the subscriber cancels Call Waiting without notifying their alarm installing company, the control panel can still send reports using the backup number.



Dialing a Call Waiting sequence on a non-Call Waiting line prevents the system from dialing the central station receiver successfully.



Example: If the central station telephone number is 555-1234, and the backup

Route Group destination is Phone 2, program Phone 2 with the following sequence: **70C5551234**.

Phone 2

Default: Blank
Selection: Up to 24 characters (do not enter [SPACE])

Refer to the explanation of **Phone 1**. This number is Phone 2, referred to in the prompts in *Section 2.3 Routing*.

Phone 3

Default: Blank
Selection: Up to 24 characters (do not enter [SPACE])

Refer to the explanation of **Phone 1**. This number is Phone 3, referred to in the prompts in *Section 2.3 Routing*.

Phone 4

Default: Blank
Selection: Up to 24 characters (do not enter [SPACE])

Refer to the explanation of **Phone 1**. This number is Phone 4, referred to in the prompts in *Section 2.3 Routing*.

2.2 Phone Parameters

The program items in this category describe panel-wide characteristics for telephone dialing, receiver format, and supervision.

Modem Format

Default: Yes
Selection: Yes or No

Yes	Modem IIIa² Communication Format: Reports identify points as 001 through 247 and passcode User ID codes as 000 through 249 at the D6500 or D6600 Receiver (unless Point/User Flag is programmed Yes; refer to the Point/User Flag prompt in this section). When reporting point events, Modem IIIa ² Communication Format also sends point text to the D6500 or D6600 as programmed in Point Assignments.
No	ANSI-SIA Contact ID

Central Station Receiver Format for Transmission of Reports: Modem format provides many reporting advantages over the Contact ID format. Refer to the *D6500 Report Directory* (P/N: 74-04651-001) for more information about the effect of reporting formats.



Modem Format must be set to Yes when sending events over a network to a D6600 Receiver.

Point/User Flag

Default: Yes	
Selection: Yes or No	
Yes	The control panel sends a flag with each report telling the D6500 or D6600 to convert point numbers and User ID numbers to COMEX format. Refer to <i>Table 7</i> and <i>Table 8</i> for conversion information. When this parameter is programmed Yes , points and User ID numbers are converted, regardless of the programming of the D6500 or D6600 Receiver for output to the computer system. Refer to <i>Appendix C</i> in the <i>Conettix D6600/D6100 Receiver/Gateway Computer Interface Manual</i> (P/N: 4998122703).
No	The control panel does not send the flag. The D6500 or D6600 outputs point numbers as 001 to 247 (rather than 100 to 732) and User ID numbers as 000 to 249 (rather than 000 to F08), as indicated in <i>Table 7</i> and <i>Table 8</i> .

This program item determines how point and User ID numbers are presented at the D6500 or D6600 display, printer, and computer RS-232 output.

When **Modem Format** is Yes, the control panel sends expanded Bosch Modem IIIa² Communication Format reports to the D6500 or D6600. If your central station data files are not set up for point and User ID number reporting, you can use this program item to convert these numbers to COMEX Reports.

When **Modem Format** is Yes, the control panel sends expanded Bosch Modem IIIa² Communication Format Reports to the receiver. **Point/User Flag** affects Bosch Modem IIIa² Communication Format data as shown in *Table 7*. The Bosch Security Systems, Inc. D6500 or D6600 Receiver adds the leading zero in the User ID number with **Point/User Flag** programmed No.

Table 7: Modem IIIa² Communication Format Data - User ID Numbers

Point/User Flag NO	Point/User Flag YES
000	000
001 to 005	001 to 005
006 to 013	601 to 608
014 to 021	701 to 708
022 to 029	801 to 808
030 to 037	B01 to B08
038 to 045	C01 to C08
046 to 053	D01 to D08
054 to 061	E01 to E08
062 to 069	F01 to F08
070 to 249	000

Table 8: Modem IIIa² Communication Format Data - Point Numbers

Point/User Flag NO	Point/User Flag YES
001 to 008	100 to 800
009 to 024	101 to 116
025 to 040	201 to 216
041 to 056	301 to 316
057 to 072	401 to 416
073 to 088	501 to 516
089 to 104	601 to 616
105 to 120	701 to 716
121 to 136	801 to 816
153 to 168	217 to 232
169 to 184	317 to 332
185 to 200	417 to 432
201 to 216	517 to 532
217 to 232	617 to 632
233 - 247	717 to 731

2.2.1 Special Point/User Reporting

Independent Zone Control Notice: When using Independent Zone Controls (IZC) to send Opening/Closing Reports by point, do not duplicate reporting independent point numbers with User ID Reports (refer to *Section 3.1 Passcode or Token Worksheet* on page 82). For example: If an IZC is connected to Point 8, do not use User ID 8.

D6000: Opening/Closing User ID numbers are identified at the receiver as zones (same identification as independent points). Refer to *Table 9*.

Table 9: D6000 User IDs and Zones

User ID Number	Zone	User ID Number	Zone
1	B	91	1
2	C	92	2
3	D	93	3
4	E	04	4
5	F	95	5
6	6	96	0
7	7		
8	8		

DTMF Dialing

Default:	Yes
Selection:	Yes or No
Yes	Dials the programmed phone number(s) using DTMF.
No	Pulse dialing only.

Use dual-tone multi-frequency (DTMF) to dial the central station receiver phone number(s) for event reports, or to dial the remote programming software (RPS).

Phone Supv Time

Default:	Blank
Selection:	Blank or 10 to 240
Blank	No phone line supervision.
10 to 240	Enter the number of seconds (in 10 sec increments) you wish to wait before indicating trouble. After a faulted phone line restores, it takes the same amount of time to start restoral responses.

Phone line trouble responses: Keypads display SERVC PH LINE # to indicate which phone line failed. The keypad initiates a trouble tone if **Buzz on Fail** is Yes and **CC Trouble Tone** is Yes.

With dual phone lines (using the D928 Module), the restored phone line handles all messages regardless of the phone line's number.

Phone, Trouble, and Restoral Events report when they occur. They report also when a Diagnostic Report is initiated from a keypad or by a Sked.



To meet UL 864 requirements, set this parameter to a non-zero value.

Alarm On Fail

Default:	No
Selection:	Yes or No
Yes	Generate alarm responses when a phone line fails.
No	Phone failures report as trouble responses for Area 1 or the account number associated with Area 1.



To meet UL 864 requirements, set this parameter to **No**.



Phone Supv Time must be programmed to use this feature.

Phone Failure Alarm Responses: The Alarm Bell relay for Area 1 activates. All Phone Event messages report as Area 1 and the account number for Area 1.

Buzz on Fail

Default: No	
Selection: Yes or No	
Yes	Generate panel-wide trouble tones and display PHONE FAIL # at keypads when a Phone Fail Event occurs.
No	Does not generate trouble tones at keypads when a Phone Fail Event occurs. PHONE FAIL # still displays.



To meet UL 864 requirements, set this parameter to **Yes**.



Phone Supv Time must be programmed to use this feature.

When **Buzz on Fail** is Yes, users can disable the resulting trouble tone on individual keypads by setting **CC# Trouble Tone** to No.

Two Phone Lines

Default: No	
Selection: Yes or No	
Yes	The D928 Dual Phone Line Module is installed. The LEDs on the D928 light to indicate primary or secondary line trouble and COMM FAIL.
No	D928 Dual Phone Line Module is not installed.



When using two telephone lines, set this parameter to **Yes** to meet UL 864 requirements.



Program **Phone Supv Time** when using two phone lines.

BFSK Duress Code

Default: 0	
Selection: 0 to 9	
This prompt is not supported in GV3 Series control panels. Leave the value set to the factory default of 0.	

Expand Test Rpt

Default: No	
Selection: Yes or No	
Yes	Off-normal events listed in Routing Group Test Reports are reported to the central station.
No	Off-normal conditions for the events listed in the Routing Group Test Reports at test time are not reported.

Use this program item to add system event information to scheduled Test Reports. Refer to *Section 5.2 Skeds* on page 114.



This parameter relates to Sked Function Code 9 (Test Report) because it allows a Sked to send Expanded Test Report information. **Expand Test Rpt** does **not** affect Sked Function Codes 28 (Expanded Off-Normal Test Report) and 29 (Non-Expanded Off-Normal Test Report).

2.3 Routing

Use routing to select full or partial groups of events that report to up to four different destinations. Routing includes choosing the most important destination (route number), reporting the events to a single or multiple destination, and selecting a backup destination if the events fail.

2.3.1 Called Party Disconnect

Telephone companies provide called party disconnect to allow the called party to terminate a call. The called party must go on hook (hang up) for a fixed interval before a dial tone is available for a new call. This interval varies with telephone company equipment. D9412GV3/D7412GV3 firmware allows for called party disconnect by adding a 35-sec on-hook interval to the dial-tone detect function. If the control panel does not detect a dial tone in 7 sec, it puts the phone line on hook for 35 sec to activate called party disconnect. The phone line goes off hook and begins a 7-sec dial tone detect. If no dial tone is detected, the control panel dials the number anyway. Each time the number is dialed, the control panel records this as an attempt. After ten attempts, the control panel enters communications failure and Comm Fail Route # appears on the keypads.

2.3.2 Route Number Groups: Which Has the Highest Priority?

To program a group, first choose a route number. The lower the route number, the higher priority that group has (for example, events reported for Route 1 have a higher priority than Routes 2, 3, or 4 if each group tries to send a message at the same time). The priority of the route numbers becomes important when programming duplicate reports or choosing the events you want to report first regardless of the number of events that must report to multiple groups. Route 1 group primary device is the first destination the control panel attempts to dial if an event in that group must be reported. If the control panel is idle, any event generated for any group starts a dialing sequence.

2.3.3 Programming Primary and Backup Destinations

Each route number has an **R# Primary Device** and an **R# Backup Device**. In typical applications where two phone numbers are programmed, the **R# Primary Device** destination is the phone number that the route group attempts to dial first. If the **R# Primary Device** destination does not connect to the central station receiver after two dialing attempts, the control panel dials the **R# Backup Device** destination.

You can also program the control panel so that the **R# Primary Device** or the **R# Backup Device** uses an SDI device, such as a D4020 Network Interface Module.

2.3.4 Enhanced Routing

The D9412GV3 and D7412GV3 allow events to be sent to up to four additional SDI Paths. The network interface modules (NIMs) connect directly to the SDI Bus and occupies SDI Address 88 or 92. For additional information regarding the specific programming requirements for enhanced communications, refer to *Section 2.4 Enhanced Routing* on page 24 and *Section 6.5 Programming Path Numbers and IP Addresses for Enhanced Communications* on page 134.

2.3.5 Programming a Duplicate Report

Select **Yes** for each available route number to allow an event within a group to send a report to multiple groups. For instance, if fire alarms are programmed for Route Group 1 and Route Group 2, a fire alarm sends a report first to Route Group 1, followed by a duplicate report to Route Group 2.

2.3.6 Routing Destination Communication Failures

When the R# Primary Device fails to connect to the central station receiver after two attempts, the R# Backup Device phone number will be dialed. The central station will receive the original event with a COMM TROUBLE PHONE # = (1, 2, 3, or 4) message added. This event does not occur if there is no backup phone number. COMM RESTORE events are generated.

If the **R# Primary Device** is an SDI Path, the central station receives the original event with a COMM TROUBLE RG8 SDI## event modifier. Refer to *Table 10*.

Table 10: SDI Path Number by Device

Path	1	2	3	4
SDI 88	88	89	90	91
SDI 92	92	93	94	95

When all attempts to both the R# Primary Device and R# Backup Device fail, a COMM FAIL RG# event is generated. COMM RESTORE RG# events are generated when a successful report (via phone or IP) or a successful poll (via IP) is sent over either route within the failed Route Group, even if the report is sent using a different Route Group.

The same COMM TROUBLE conditions occur if the control panel does not receive a positive acknowledgement to a poll from the central station receiver after the configured number of retries. Refer to *Path # Poll Rate* on page 135.

2.3.7 Message Prioritization within a Route Number

The D9412GV3/D7412GV3 Control Panels meet the digital reporting requirements for UL 864. Fire Alarm Events have the highest priority and reports are sent first for each group. Other events are sent in the following order: Panic, Duress, Medical, Intrusion Alarm, Supervisory, and all troubles and restorals.



To comply with NFPA and UL 864, program **Route 1** to send a report of only Fire Alarm Events to ensure the fastest reporting time.

2.3.8 Dialing Attempts

The control panel makes up to ten dialing attempts using the primary and backup devices within a route group. If unsuccessful, it sends a Comm Fail Report. The dialing attempts occur in the following sequence:

1. Primary device
2. Primary device
3. Backup device
4. Backup device
5. Primary device
6. Backup device
7. Primary device
8. Backup device
9. Primary device
10. Backup device

When only one destination is programmed, the control panel makes ten attempts to contact that destination. When reporting via phone, each group takes approximately 10 min to go into Comm Fail.

Route

Default: 1	
Selection: 1 to 4	
1	First group sent
2	Second group sent
3	Third group sent
4	Fourth group sent

Enter the number specifying the route group to program. The route represents the group you wish to send a group of reports. Group 1 is the first group to send a report and Group 4 is the last group to send a report. Each group has a primary and a backup device. The primary device is the first (most important) destination used to reach the programmed route within this group. The backup device is used if the primary device fails.

R# Primary Device

Default: Blank	
Selection: Blank, 1 to 4	
1	Phone 1 or SDI Path 1 is this group's primary destination.
2	Phone 2 or SDI Path 2 is this group's primary destination.
3	Phone 3 or SDI Path 3 is this group's primary destination.
4	Phone 4 or SDI Path 4 is this group's primary destination.



To meet UL 864 requirements for Central Station and Remote Station applications, program a **Primary Device**.

Enter the number specifying the primary device.

R# Backup Device

Default: Blank	
Selection: Blank, 1 to 4	
1	Phone 1 or SDI Path 1 is this group's backup destination if the primary destination fails.
2	Phone 2 or SDI Path 2 is this group's backup destination if the primary destination fails.
3	Phone 3 or SDI Path 3 is this group's backup destination if the primary destination fails.
4	Phone 4 or SDI Path 4 is this group's backup destination if the primary destination fails.



To meet UL 864 requirements for Central Station and Remote Station applications, program a **Backup Device**.

Enter the number specifying the backup device. The backup device is used when the primary device fails to reach the programmed destination.

View Events?

Default: No	
Selection: Yes or No	
Yes	Access each routing group and program individual events for this

	route group only (D5200).
No	Continue programming without viewing individual groups.

The D5200 Programmer reveals the following sub-prompts. Leaving **View Events?** as **No** allows the user to ignore a large area of programming that might not need to be changed.

Fire Reports



To meet UL 864 requirements for Central Station and Remote Station applications, enable **Fire Reports**.

Selecting **Yes** enables a report to be sent when the event occurs.

Table 11: Fire Reports

Report	Selections	Report Description
R# Fire Alarm	Yes, No	Fire Event
R# Fire Restore (Alarm)	Yes, No	Fire restoral from alarm
R# Fire Missing	Yes, No	Missing Fire point
R# Fire Trouble	Yes, No	Fire trouble
R# Fire Supervis	Yes, No	Fire supervision
R# Fire Restore (T/M/S)	Yes, No	Fire restoral from trouble, missing, or bypass
R# Fire Cancel	Yes, No	Canceled fire alarm
R# Fire Sup Miss	Yes, No	Fire supervisory missing
R# Fire Supv Rest	Yes, No	Restorals from Fire Supervision

Burglar Reports

Select **Yes** to send a report when the event occurs.

Table 12: Burglar Reports

Report	Selections	Report Description
R# Alarm	Yes, No	Burglar Alarm Event
R# Burg Restore	Yes, No	Non-fire restoral from trouble, missing, or supervisory

R# Duress	Yes, No	Duress
R# Missing Alarm	Yes, No	Missing Alarm point
R# Usr Code Tmpr	Yes, No	User code tamper
R# Trouble Rpt	Yes, No	Trouble Event
R# Missing Trbl	Yes, No	Missing Trouble Event
R# Non Fire Suprv	Yes, No	Non-fire Supervision Event
R# Pt Bus Fail	Yes, No	Point bus failure
R# Pt Bus Rstl	Yes, No	Restoral of point bus after failure
R# Non Fire Cncl	Yes, No	Canceled non-fire alarm
R# Alarm Restore	Yes, No	Non-fire restoral from alarm
R# Sup Missing	Yes, No	Supervisory missing
R# Unverified Evt	Yes, No	Unverified Events for Cross Points



R# Unverified Evt is sent when a single point programmed in Cross Point Group faults into an alarm condition, then restores before the Cross Point Time elapses.

R# Unverified Evt encompasses both Fire and Non-fire points, but is not related to the **A# Verify Time** used for smoke detectors.



The GV3 Series control panels log a Ground Fault Event as Trouble Point 256.



Restoral Reports are not sent if the control panel resets after a point is bypassed and then unbypassed. This is true for both Fire and Non-fire points.

User Reports

Selecting **Yes** enables a report to be sent when the event occurs.

Table 13: User Reports

Report	Selections	Report Description
R# Point Bypass	Yes, No	Point Bypass Event

R# Forced Point	Yes, No	Forced Point Event
R# Point Open	Yes, No	Point Opening Event
R# Point Close	Yes, No	Point Closing Event
R# Forced Arm	Yes, No	Point Force Armed
R# Fail To Open	Yes, No	Fail to Open Event
R# Fail To Close	Yes, No	Fail to Close Event
R# Ext Clos Tm	Yes, No	Extend Close Time Event
R# Opening Rpt	Yes, No	Opening Events
R# Forced Close	Yes, No	Point Forced Close Event
R# Closing Rpt	Yes, No	Closing Events
R# FC Perim Inst	Yes, No	Forced Close Perimeter Instant Armed Event
R# FC Perim Delay	Yes, No	Forced Close Perimeter Delay Armed Event
R# Perim Inst Arm	Yes, No	Perimeter Instant Armed Event
R# Perim Delay Arm	Yes, No	Perimeter Delay Armed Event
R# Send User Text	Yes, No	User text

Test Reports



To meet UL 864 requirements for Central Station and Remote Station applications, enable **Test Reports**.

Sending Test Reports

Automatic: To send a single Test Report (**R# Test Report**) automatically, enable Sked Function Code #9 (Test Report) in the Skeds section of the program. Refer to *Table 14*.

Manual: To send a single Test Report manually, enter [COMMAND][4][1] at the keypad. Refer to the **Send Report** prompt on page 63.

To expand this Test Report to include any off-normal point condition or other off-normal system conditions, **Expand Test Rpt** (refer to page 12) must be programmed **Yes**. Refer to the footnotes with *Table 15* on page 20 for a list of event types that are included in an expanded test report. Additionally, the expanded test report includes Summary Fire Supervisory, Summary Fire Fault, Summary Controlled Point Fault, and Summary Point Device Fault conditions.

The control panel can generate an Expanded Off-Normal Test Report by using Sked Function Code 28 or a Non-Expanded Off-Normal Test Report using Sked Function Code 29. To generate this event, one or more points must be in an off-normal state at the time the Sked executes. Expanded Off-Normal Test Reports include the Off Normal Test Report Event as well as a panel-wide summary of off-normal point and system conditions. Non-Expanded Off-Normal Test Report Events are sent only when a point is in the off-normal state but sends only the Off-Normal Test Report Event.

Sending Status Reports

Automatic: To send a Status Report automatically that includes the events shown in the footnotes in *Table 14*, enable Sked Function Code #10 in the Skeds section of the program.

Manual: To send a Status Report manually that includes the events shown in the footnotes in *Table 14*, enter [COMMAND][4][2] at the keypad. Refer to the **Send Report** prompt on page 63.

Sending off-normal conditions as a Status Report following a Test Report is required by some automation systems. Sending off-normal conditions as a Non-status Report that follows a Test Report is required for other automation systems.

An off-normal condition is any point that is missing, trouble, supervisory, or in alarm. Also, points not cleared at the keypad report as off-normal.

Table 14: Test Reports

Report	Selections	Report Description
R# S: Alarm ¹	Yes , No	Status Alarm
R# S: Trouble ¹	Yes , No	Status Trouble
R# S: Supervised ²	Yes , No	Status Supervised
R# Status Report	Yes , No	Status
R# S: Open ¹	Yes , No	Status Open
R# S: Close ¹	Yes , No	Status Close
R# Test Report	Yes , No	Test
R# S: Perim Inst ¹	Yes , No	Status Perimeter Instant Arm
R# S: Perim Delay ¹	Yes , No	Status Perimeter Delay Arm
R# S: Fire Supv ²	Yes , No	Status Fire Supervision
R# S: Fire Alarm ³	Yes , No	Status Fire Alarm Report
R# S: Fire Trbl ²	Yes , No	Status Fire Trouble
R# S: Msng Fire ²	Yes , No	Status Fire Missing
R# S: MsngBurgTr ²	Yes , No	Status Burg Missing Trouble
R# S: MsngBurgAl ²	Yes , No	Status Burg Missing Alarm
R# S: FireSpMsng ²	Yes , No	Status Fire Supervision Missing
R# S: SuperMsng ²	Yes , No	Status Non-fire Supervision Missing
R# S: DrLeftOpen ²	Yes , No	Status Door Left Open
<p>1 Information about this condition is sent with a Status Report.</p> <p>2 Information about this condition is sent as S: Trouble Event with a Status Report.</p> <p>3 Information about this condition is sent as S: Alarm Event with a Status Report.</p>		

Diag Reports

Selecting **Yes** enables sending a report when the event occurs. If the off-normal state of the events indicated by footnote 1 in *Table 15* on page 20 still exists, the events report when a Test Report is enabled and **Expanded Test Rpt** is programmed **Yes**. Refer to the **Test Reports** sub-prompt in *Section 2.3.8 Dialing Attempts* on page 17.

Table 15: Diagnostic Reports

Report	Selections	Report Description
R# SDI Dev Fail ¹	Yes , No	SDI device failure
R# SDI Dev Rstl	Yes , No	Restoral of SDI device failure
R# Watchdog Rset	Yes , No	Watchdog Reset Event
R# ParaChksmFail	Yes , No	Parameter checksum failure
R# Reboot	Yes , No	Reboot Event
R# Ph Line Fail ¹	Yes , No	Failure of phone line
R# Ph Line Rstl	Yes , No	Restoral of phone line after failure
R# AC Fail ^{1, 2}	Yes , No	Failure of AC power to control panel
R# AC Restorl ²	Yes , No	Restoral of AC power to control panel after failure
R# Batt Missing ^{1, 2}	Yes , No	Battery Missing Detection Event
R# Battery Low ^{1, 2}	Yes , No	Low battery power
R# Battery Rstl ²	Yes , No	Restoral of battery power to control panel after Missing or Low Event
R# Rt Comm Fail ^{1, 3}	Yes , No	Failure to send report to specific route
R# Rt Comm Rstl	Yes , No	Restoral of communication to specific route after a failure

Table 15: Diagnostic Reports (Continued)

Report	Selections	Report Description
R# Checksum Fail	Yes , No	Checksum Fail Event
R# Network Fail ⁴	Yes, No	Failure of network
R# Network Rest ⁴	Yes, No	Restoral of network
R# Network Cond ⁴	Yes, No	Condition of network

1 This event is included in the Expanded Test Report when an off-normal condition exists..

2 To meet UL 864 requirements for Central Station and Remote Station applications, enable **AC Fail**, **Battery Missing**, **Low Battery**, **Battery Restoral**, and **AC Restoral** reports.

3 This event covers Comm Fail Route Group and Comm Fail Phone. If enabled, both events are sent; if disabled, neither event is sent

4 This event is reserved for future use.



Enable Rt Comm Fail and Rt Comm Restore in only one route group.

Relay Reports

Selecting **Yes** enables sending a report when the event occurs.

Table 16: Relay Reports

Report	Selections	Report Description
R# Sensor Reset	Yes , No	Sensor Reset Event
R# Relay Set	Yes , No	Relay Set Event
R# Relay Reset	Yes , No	Relay Reset Event



When activating an on-board relay using remote automation software, the D9412GV3 and D7412GV3 Control Panels log and print the resulting event as:

Relay 250 (Relay A)
Relay 251 (Relay B)
Relay 252 (Relay C)

AutoFunc Reports

The following prompts support customized routing of Auto Function Reports. Selecting **Yes** enables a report to be sent when the event occurs.

Table 17: Auto-Function Reports

Report	Selections	Report Description
R# Sked Executed	Yes , No	Sked Executed Event
R# Sked Changed	Yes , No	Sked Changed Event
R# Execute Fail	Yes , No	Fail to Execute Event

RPS Reports

Selecting **Yes** enables sending a report when the RPS Passcode Event occurs.



"RPS Access Fail" might indicate a wrong RPS passcode when communicating with the control panel, or a valid RPS session was abnormally terminated. "Remote Reset" indicates a Reset command was issued from RPS. "Bad Call to RPS" indicates that control panel called RPS, but was unable to connect.

Table 18: RPS Reports

Report	Selections	Report Description
R# Log Threshold	Yes , No	Event log threshold reached
R# Log Overflow	Yes , No	Log is full, old events are overwritten
R# Para Changed	Yes , No	RPS Parameter Change Event
R# RPS OK	Yes , No	Successful RPS Access Event
R# RPS Fail	Yes , No	Failed Access RPS Event
R# Remote Reset	Yes , No	Remote Reset Event
R# Program OK	Yes , No	Successful Local Programming Event
R# Program Fail	Yes , No	Failed Local Programming Event

Point Reports

Selecting **Yes** enables a report to be sent when the event occurs.

Table 19: Point Reports

Report	Selections	Report Description
R# Service Start	Yes , No	Reorts Service Walk Test Start Event
R# Service End	Yes , No	Service Walk Test End Event
R# Fire Walk St	Yes , No	Fire Walk Start Event
R# Fire Walk End	Yes , No	Fire Walk End Event
R# Walk Test St	Yes , No	Walk Test Start Event for Walk Test and Invisible Walk Test
R# Walk Test End	Yes , No	Walk Test End Event for Walk Test and Invisible Walk Test
R# Extra Point	Yes, No	Extra Point Event
R# Send Point Text [¶]	Yes , No	Point Text
R# RF Low Bat	Yes, No	Low battery conditions for RF points
R# RF Low Bat Res	Yes, No	Low battery restoral conditions for RF points
[¶] Point text is always transmitted when using network applications.		

User Chng Reports

Selecting **Yes** enables a report to be sent when the event occurs.

Table 20: User Change Reports

Report	Selections	Report Description
R# Date Changed	Yes, No	Date Change Event
R# Time Changed	Yes, No	Time Change Event
R# Delete User ¹	Yes, No	Delete User Code Event
R# User Code Chg	Yes, No	User Passcode Add or Change Event
R# Area Watch	Yes, No	Start and end of area watch
R# Card Assigned	Yes, No	Card Assigned to User Event
R# Change Level	Yes, No	Access Control Level Change Event

¹ With R# Delete User Events, the control panel always uses the account number from Area 1.

Access Reports

Selecting **Yes** enables a report to be sent when the event occurs.



Access Granted, No Entry, Request to Enter (RTE) and Request to Exit (REX) Events can be enabled or disabled by each D9210B.

Table 21: Access Reports

Report	Selections	Report Description
R# Access Granted	Yes, No	Access Granted Event
R# No Entry	Yes, No	No Entry Event
R# Door Lt Open	Yes, No	Door Left Open Event
R# Cycle Door	Yes, No	Open Door Event
R# Door Unlocked	Yes, No	Unlock Door Event
R# Door Secure	Yes, No	Secure Door Event
R# Door Request	Yes, No	RTE or REX Event
R# Door Locked	Yes, No	Locked Door Event

2.4 Enhanced Routing

Enhanced routing allows the control panels to determine if events are routed over one of the following:

- Standard telephone lines
- Local-area network (LAN)
- Wide-area network (WAN)
- General Packet Radio System (GPRS)

Sending events over a LAN or WAN requires a network interface module (NIM), such as the DX4020. Sending events over GPRS requires a special NIM (ITS-DX4020-G).



Refer to *Section 6.5 Programming Path Numbers and IP Addresses for Enhanced Communications* on page 134 for details on Enhanced Communications Route path programming.

Enhanced routing also enables and disables the ability of the control panel to send events to a numeric pager.



If the installation does not require these applications, skip this section.

With enhanced routing, whether you use standard telephone lines or a NIM, you can program the control panel to send full or partial groups of events to as many as four different destinations. Routing includes:

- Choosing the most important destination
- Sending events to a single destination or to multiple destinations
- Selecting a backup destination if events fail.



When programming with a D5200 Handheld Programmer, in any one route group do not configure both the primary and backup routes to use the same network module and the same path number. A communication trouble on the primary path may cause a premature communication failure.

2.4.1 Programming a Primary and Backup Destination

Each route number has an **R# Primary Device** and an **R# Backup Device**. With enhanced communications, the **R# Primary Device** destination can be either the phone number or the path number for the SDI device, to which the route group first attempts to send the event. If the **R# Primary Device** destination fails to connect to the central station receiver after two attempts, the control panel attempts to connect with the **R# Backup Device** destination.

2.4.2 Programming a Duplicate Report

To send an event within a group to multiple groups, program the event as **Yes** for each route number available. For example, programming fire alarms for Route Group 1 and Route Group 2 sends a fire alarm report first to Route Group 1, followed by a duplicate report to Route Group 2.

Section 2.4 Enhanced Routing on page 24 determines the route groups and which destinations within the route groups use network interface modules (NIMs) for reporting purposes. A single NIM can send events to as many as four different destinations.

For example, if you want to send events using Route Group 1 over a LAN, WAN or GPRS as your primary destination, and use a standard telephone line as your backup destination, program the following sections:

- Routing (*Section 2.3 Routing* on page 16)
 1. Select Route Group 1
 2. Program a 1 for Primary Destination
 3. Program a 1 for Backup Destination
 4. Enable all applicable events to be included in Route Group 1.
- Phone (*Section 2.1 Phone* on page 11)
 1. Select Phone 1.
 2. Program Phone 1 with the applicable central station receiver phone number.
- Enhanced Routing (*Section 2.4 Enhanced Routing* on page 24)
 1. Enter **Yes** for **RG1 Primary SDI 88**. This parameter tells the control panel to send the events to the network interface module (NIM) installed at SDI 88 using the IP Address in path 1.
 2. Enter **No** for **RG1 Backup SDI 88** and **No** for **RG1 Backup SDI 92**. These parameters tell the control panel to use the phone line to send events if the primary destination fails after one or two attempts.

Because you are using an SDI Path to send events, you must also program the applicable items in *Section 6.5 Programming Path Numbers and IP Addresses for Enhanced Communications* on page 134.

**UL 864 Enhanced Communication Path Report Prioritization:**

To ensure that high priority events such as Fire Alarms are reported before any other queued event reports, use Route Groups 1 and 2. The lower numbered route groups are higher priority than the higher numbered route groups. For example, the following route groups are listed from highest priority to lowest priority: RG1 RG2 RG3 RG4.

UL 864 Enhanced Communication Path Supervision:

To detect and locally annunciate a break in an Enhanced Communication Path in less than 200 sec, program no more than two Enhanced Communication Paths in no more than two Route Groups. Use the following settings for both Enhanced Communication Paths:

Path # Poll Rate: 75 sec

Path # ACK Wait: 13 sec

Path # Retry Count: 5



If the External Modem feature is used, **RG# Primary SDI** and **RG# Backup SDI** must be set to **No**. The control panel supports either enhanced communication or external modem, but not both at the same time.

RG# Primary SDI 88

Default: No

Selection: Yes or No

This parameter determines if the primary destination for Route Group 1 (2, 3 or 4) is sent to the NIM installed as SDI address 88.

RG# Backup SDI 88

Default: No

Selection: Yes or No

This parameter determines if the backup destination for Route Group 1 (2, 3 or 4) is sent to the NIM installed as SDI address 88.

RG# Primary SDI 92

Default: No

Selection: Yes or No

This parameter determines if the primary destination for Route Group 1 (2, 3 or 4) is sent to the NIM installed as SDI address 92.

RG# Backup SDI 92

Default: No

Selection: Yes or No

This parameter determines if the backup destination for Route Group 1 (2, 3 or 4) is sent to the NIM installed as SDI address 92.



To completely disable Enhanced Routing over an SDI path, **RG# Primary SDI 88**, **RG# Backup SDI 88**, **RG# Primary SDI 92**, **RG# Backup SDI 92**, and **Enhanced Comm** prompts must be set to **No**.



The poll rate entry for the backup SDI path might need to increase because of heavy traffic on the network or excessive signals generated at the same time. All Comm prompts must be set to **No**.

RG# Primary Pager

Default: No

Selection: Yes or No

This parameter determines if this route group sends events to a numeric pager. To send events to a numeric pager, a phone number must also be programmed in the route group's primary destination.

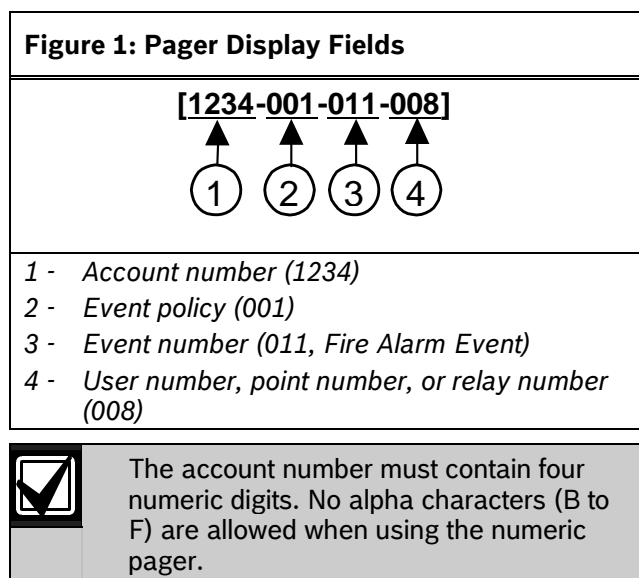


If programming the control panel to dial a numeric pager, choose its route group carefully. Place events being sent to a central station in a route group class with a lower number than the numbers of the events in the route group for the numeric pager.

2.4.3 Numeric Pager Capability

The D9412GV3 and D7412GV3 Control Panels can send most events to a numeric pager. Any time an event is generated and routed to a numeric pager, the control panel calls the numeric pager once for each message in the queue. To enable the pager, program the primary phone number and the backup phone number to the numeric pager's phone number in any of the four route groups. Then select which events to route to the numeric pager within the selected route group.

Up to four event fields can be shown in the pager message. Refer to *Figure 1*.



Programming the Pager Phone Number

To program the pager phone number, enter the number used to reach the pager, followed by pauses. Entering C creates a 3-sec pause (example: 5552341CCC.)

Experiment with the number of pauses you add after the page phone number. Each pause equals 3 sec. Try calling the pager yourself first and listening to the length of time it takes to get a beep allowing you to enter touch-tone information. This length is what you must program after the pager's phone number in *Section 2.1 Phone* on page 11. If you need a longer pause, enter D after the number. Each D equals 7 sec.

Using “#” characters in the phone number affects the event's display on the pager:

- **No “#” characters in phone number:** Dashes appear in the display [1234-001-011-008].
- **One “#” character in phone number:** Dashes are replaced by zeros [1234000100110008].
- **Two or more “#” characters in phone number:** Dashes appear in the display [1234-001-011-008].

For example, if the phone number 2773074#CC (seven-digit pager phone number followed by “#” and two pauses) is programmed, the pager message appears as follows: [1234000100110008] (dashes are replaced by zeros).

If the “#” is not placed in the phone number, the message appears as follows: [1234-001-011-008]

A user might not want all four fields to show in the pager message. Entering “*” characters in the phone number allows the user to select the number of fields to show in the pager message. To limit the number of fields shown in the pager message, enter the appropriate number of “*” characters in the phone number as shown below:

- **Zero “*” characters in phone number:** Shows all four fields.
- **One “*” character in phone number:** Shows first field only.
- **Two “*” characters in phone number:** Shows first two fields.
- **Three “*” characters in phone number:** Shows first three fields.
- **Four or more “*” characters in phone number:** Shows all four fields.

For example, the phone number 2773074***CC (seven digit pager phone number followed by three asterisks and two pauses) produces the following pager display: [1234-001-011] (three fields display at the pager).

Table 22 shows the description of each event, its priority, and event number.

Table 22: Event Descriptions, Priorities, and Numbers

Event Description	Event Priority	Event Number
Fire Alarm	001	011
Fire Alarm Restoral	005	014
Fire Missing	005	013
Fire Trouble	005	012
Fire Supervision	005	124
Fire Restoral (after Tbl, Msg, Bypass)	005	015
Fire Cancel	004	027
Fire Supervision Missing	005	146
Fire Supervision Restore	005	123
Alarm Report	003	016
Duress	002	004
Missing Alarm	006	019
User Code Tamper	008	055
Trouble Report	006	017
Missing Trouble	008	020
Non-Fire Supervision	006	078
Point Bus Fail	006	024
Point Bus Restoral	006	091
Non-Fire Cancel	004	045
Alarm Restore	006	026
Supervision Missing	008	147
Unverified Event	006	169
Point Bypass/Command Bypass	007	007
Forced Point	007	008
Point Opening	008	021
Point Closing	008	022
Was Force Armed	007	034
Fail To Open	008	040
Fail To Close	008	041
Extend Close Time	008	044
Opening Report	008	047
Forced Close	007	048
Closing Report	008	050

Table 22: Event Descriptions, Priorities, and Numbers (Continued)

Event Description	Event Priority	Event Number
Forced Close Perim Instant	007	084
Forced Close Perim Delay	007	085
Perimeter Instant Armed	008	088
Perimeter Delay Armed	008	089
Send User Text	n/a	n/a
S: Alarm	n/a	n/a
S: Trouble	n/a	n/a
S: Supervision	n/a	n/a
Status Report	008	035
S: Open	n/a	n/a
S: Close	n/a	n/a
Test Report	008	051
S: Perimeter Instant	n/a	n/a
S: Perimeter Delay	n/a	n/a
S: Fire Supervision	n/a	n/a
S: Fire Alarm	n/a	n/a
S: Fire Trouble	n/a	n/a
S: Missing Fire (Trouble)	n/a	n/a
S: Missing Burglary ((Trouble)	n/a	n/a
S: Missing Burglary (Alarm)	n/a	n/a
S: Fire Supervision Missing	n/a	n/a
S: Burglary Supervision Missing	n/a	n/a
S: Door Left Open	n/a	n/a
SDI Device Failure*	004	070
SDI Device Restoral*	008	071
Watchdog Reset	004	077
Parameter Checksum Fail	n/a	n/a
Reboot	008	082
Phone Line Fail	004	068
Phone Line Restoral	008	069
AC Failure	004	072
AC Restoral	008	073
Battery Missing	004	074
Battery Low	004	075
Battery Restoral	008	076
Route Comm Fail	004	066
Route Comm Restore	008	067
Checksum Fail	n/a	n/a
Sensor Reset	007	031
Relay Set	007	032
Relay Reset	007	033
Sked Executed	007	057
Sked Changed	007	058
Fail to Execute	008	151
Event Log Threshold	008	052
Event Log Overflow	008	053

* SDI Device number is not reported when using pager format.

Table 22: Event Descriptions, Priorities, and Numbers, continued

Event Description	Event Priority	Event Number
Parameters Changed	008	054
RPS Access OK	008	064
RPS Access Fail	008	065
Remote Reset	008	079
Program Access OK	n/a	n/a
Program Access Fail	n/a	n/a
Service Start	008	029
Service End	008	030
Fire Walk Start	008	036
Fire Walk End	008	037
Walk Test Start	008	038
Walk Test End	008	039
Extra Point	008	023
Send Point Text	n/a	n/a
RF Low Battery	006	093
RF Battery Restore	006	094
Date Changed	008	059
Time Changed	008	060
Delete User	008	090
User Code Change	008	056
Area Watch	008	042
Card Assigned	008	110
Change Level	007	061
Access Granted	008	003
No Entry	008	115
Door Left Open	008	116
Cycle Door	008	112
Door Unlocked	008	113
Door Secure	008	114
Door Request	008	117
Door Locked	008	145
User Alarm COMMAND 7	002	005
User Alarm COMMAND 9	002	006

2.5 Power Supervision

AC Fail Time

Default: 1

Selection: 1 to 90 (Blank and 0 are invalid)

Program the amount of time that AC power must be off before the control panel responds to the AC failure. The response to restoral of AC power is delayed for the same amount of time. The control panel always monitors AC. The response to this prompt is the actuation of the relay programmed in the Panel-Wide Relays prompt **AC Failure** (refer to *Section 2.13.2 Panel-Wide Relays* on page 81) and the AC Fail report enabled by the **AC Fail/Res Rpt** prompt. Local annunciation of an AC failuter is controlled by the **AC Fail Display** prompt.



UL 864 requirements, Section 50.2.1.b states: "A trouble signal shall be transmitted for remote station, central station, and proprietary-type protected premises units after a delay of between 60 and 180 min.

Exception: Products are not prohibited from providing capability of selecting that the primary power failure trouble signal transmission be delayed other time periods, including no delay, provided the 60 – 180 min delay is also included."

To meet UL 864 requirements, program **AC Fail Time** with 61, 63, 65, ... (odd numbered values), and 89. Always check with the Authority Having Jurisdiction for local requirements.

When you program **AC Fail Time**, if the second digit is:

- 1, 3, 5, 7, or 9 (such as 3, 5, 11, 13, 15, 21, and so on): The **AC Fail Time** interval is in minutes.
- 2, 4, 6, 8, or 0 (such as 2, 4, 6, 10, 12, 20, 22, and so on): The AC Fail Time interval is in seconds.



For the following items to be true, **AC Fail/Res Rpt** must be programmed as **Yes** and **AC Tag Along** must be programmed as **No**.

When you program **AC Fail Time**, if the second digit is:

- **1, 3, or 5 (such as 3, 5, 11, 13, 15, 21, and so on):** The AC Fail Time interval is in minutes and an AC Fail Event is sent after the loss of AC for this amount of time.
No additional AC Fail Events are sent after 6 hours or 12 hours.
- **2, 4, or 6 (such as 2, 4, 6, 12, 14, 16, 22, 24, 26, and so on):** The AC Fail Time interval is in seconds and an AC Fail Event is sent after the loss of AC for this amount of time.
No additional AC Fail Events are sent after 6 hours or 12 hours.
- **7 (such as 7, 17, 27, 37, and so on):** The AC Fail Time interval is in minutes and an AC Fail Event is sent after the loss of AC for this amount of time.
An additional AC Fail Event is sent after 6 hours if the AC Fail condition is still present.
- **8 (such as 8, 18, 28, 38, and so on):** The AC Fail Time interval is in seconds and an AC Fail Event is sent after the loss of AC for this amount of time.
An additional AC Fail Event is sent after 6 hours if the AC Fail condition is still present.
- **9 (such as 9, 19, 29, 39, and so on):** The AC Fail Time interval is in minutes and an AC Fail Event is sent after the loss of AC for this amount of time.
An additional AC Fail Event is sent after 12 hours if the AC Fail condition is still present.
- **0 (such as 10, 20, 30, and so on):** The AC Fail Time interval is in seconds and an AC Fail Event is sent after the loss of AC for this amount of time.
An additional AC Fail Event is sent after 12 hours if the AC Fail condition is still present.

For the following items to be true, **AC Fail/Res Rpt** must be programmed as **No** and **AC Tag Along** must also be programmed as **No**.

When you program **AC Fail Time**, if the second digit is:

- **1, 3, or 5 (such as 3, 5, 11, 13, 15, 21, and so on):** The AC Fail Time interval is in minutes. No AC Fail or AC Restoral Events are sent.
- **2, 4, or 6 (such as 2, 4, 6, 12, 14, 16, 22, 24, 26, and so on):** The AC Fail Time interval is in seconds. No AC Fail or AC Restoral Events are sent.

- **7 (such as 7, 17, 27, 37, and so on):** The AC Fail Time interval is in minutes. An AC Fail Event is only sent after 6 hours if the AC Fail condition is still present.
- **8 (such as 8, 18, 28, 38, and so on):** The AC Fail Time interval is in seconds. An AC Fail Event is only sent after 6 hours if the AC Fail condition is still present.
- **9 (such as 9, 19, 29, 39, and so on):** The AC Fail Time interval is in minutes. An AC Fail Event is only sent after 12 hours if the AC Fail condition is still present.
- **0 (such as 10, 20, 30, and so on):** The AC Fail Time interval is in seconds. An AC Fail Event is sent after 12 hours only if the AC Fail condition is still present.



To eliminate AC Reporting, **AC Tag Along** and **AC Fail/Res Rpt** must be programmed as **No** and the second digit of the AC Fail Time must be a 1, 2, 3, 4, 5, or 6.

AC Fail Display

Default: 60 sec
Selection: 10 to 300 sec (in 5-sec increments)

Program the length of time the AC power must be off before the message SERVC AC FAIL shows on the keypads. The response to restoral of AC power is delayed for the same amount of time.

AC Fail/Res Rpt

Default: No
Selection: Yes or No

Yes	Send AC Fail and AC Restoral Reports.
No	Does not send AC Fail and AC Restoral Reports.

AC Power Supervision Reports are sent to the central station and local printer at the time programmed for **AC Fail Time**.

AC Tag Along

Default:	Yes
Selection:	Yes or No
Yes	Send AC messages as tag along events.
No	Do not send AC messages as tag along events.

Send AC Reports only if any other event occurs while AC is off-normal.



If **AC Tag Along** is set to **Yes** and a subsequent event is generated, the AC Fail Event is sent first, before sending any subsequent events.



AC Tag Along is required for NFPA and UL 864 Commercial Fire systems. Be sure to program **AC Fail/Res Rpt** as **No** if **AC Tag Along** is programmed **Yes**.

AC/Battery Buzz

Default:	No
Selection:	Yes or No
Yes	Initiates panel-wide trouble tone at all keypads.
No	Does not initiate panel-wide trouble tone at keypads

Initiates a panel-wide trouble tone at keypads when AC fails or battery is low or missing. This program item does not prevent the SERVC AC FAIL or SERVC BATT LOW displays.



To comply with NFPA standards and UL 864 requirements for Commercial Fire systems, program this item as **Yes**.



If annunciating panel-wide troubles at a keypad with **CC# Scope** set to **Panel Wide** is undesirable, set **CC# Trouble Tone** to **No**. Refer to *Section 2.10 Keypad (Command Center)* on page 50 for keypad configurations.

Bat Fail/Res Rpt

Default: Yes			
Selection: Yes or No			
Yes	Battery Failure and Restoral Reports are sent to the central station. They are routed to the telephone number programmed for Power/Phone Events.		
	Modem Reports	Missing or shorted	BATTERY MISSING
		Discharged below 12.1 VDC	BATTERY LOW
No	Battery Failure and Restoral Reports are not sent to the central station.		



To comply with NFPA standards and UL 864 requirements for Commercial Fire systems, program this item as **Yes**.

2.6 Printer Parameters

Up to three D9131A Parallel Printer Interface Modules can be connected to the D9412GV3's (one printer for the D7412GV3's) SDI bus. Each printer is identified by an address of 17, 18, or 19. Options are available for Routing Reports and area assignments.

Printer Address

Default:	17
Selection:	17, 18, or 19 (only 17 is available for the D7412GV3)

Enter the printer address you are programming.

P## Area Assign

Default:	1
Selection:	1 to 8

Assign an area to the printer programmed in **Printer Address**.

P## Supervised

Default: No	
Selection: Yes or No	
Yes	Only one printer can be installed for this P## SDI address.
No	More than one unsupervised printer can be installed using this P## SDI address and the same address DIP switch setting.

Supervise this SDI address. Generate Trouble SDI ## Reports and local trouble annunciation if a problem occurs with this printer or the SDI bus.



Unsupervised printers sharing the same address setting print the same text.



Trouble SDI ## Reports are always reported as Area 1, Account 1 Events regardless of where the SDI device is assigned.



When **P## Supervised** is set to **Yes** and all Printer Event Groups (such as **P## Fire Events**, **P## Burglar Event**, or **P## Usr Chng Evt**) are set to **No**, the control panel does not generate Trouble SDI ## Reports for the printer if the D9131A becomes disconnected.

P## Scope

Default: No Printer	
Selection: No Printer, Area, Account, Panel Wide, Custom	
Panel Wide	Printer prints all designated events that occur panel-wide. A panel-wide printer can cross account boundaries.
Account	Printer prints all designated events that occur within any area with the same account number in which this printer is assigned.
Area	Printer prints all designated events that occur in the area to which this printer is assigned.
Custom	Printer prints all events occurring in areas programmed Yes for this prompt regardless of any boundary restrictions.
No Printer	No printer installed at this address. If a printer is connected, data does not print.

Press the [SPACE] bar to scroll through the selections. Press [ENTER] when the correct selection appears in the display.



The following prompts are visible **only** when you program **P## Scope** to Custom.

P## A1 [through A8] in Scope

Default: No	
Selection: Yes or No	
Yes	Include Area # Events in the scope of this printer.
No	Does not include Area # Events in the scope of this printer.

Only available if **P## Scope** is programmed Custom. This program item determines if events occurring in an area print at this printer.



Refer to the report tables in *Section 2.3 Routing* on page 16 to identify the events that print. Events programmed as **No** in Routing still print at the local printer. Individual events within the report group cannot be suppressed for events printed at the local printer.

P## Fire Events**Default:** Refer to the program record sheet**Selection:** Yes or No

Yes	All events in this group print at assigned printer.
-----	---

No	No events in this group print at assigned printer.
----	--

Use this prompt to determine whether these events print at assigned printer.

P## Burglar Event**Default:** Refer to the program record sheet**Selection:** Yes or No**P## Access Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## User Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Test Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Diag Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Auto Functions Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## RPS Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Relay Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Point Event****Default:** Refer to the program record sheet**Selection:** Yes or No**P## Usr Chng Evt****Default:** Refer to the program record sheet**Selection:** Yes or No**2.7 RPS Parameters**

Use these program items to enable remote programming software (RPS) functions in the control panel using the on-board phone connection. Two other methods of remote programming are available (external modem and LAN or WAN connection) using RPS. Refer to *Section 6.4 SDI RPS Parameters* on page 126 for more information on these types of remote programming.

2.7.1 Uploading and Downloading Reports

If the control panel is programmed to send reports in modem format, when RPS contacts the control panel and the passcode is incorrect, the control panel sends an RPS Access Fail Report to the D6500 or D6600. RPS Access Fail might indicate a wrong RPS passcode when communicating with the control panel, or a valid RPS session was abnormally terminated.

RPS ACCESS OK is sent according to phone routing when a Disconnect command is entered from RPS to terminate the call.

When a Reset Panel is used to terminate the call, a Remote Reset Report is sent to the D6500 or D6600, and an RPS ACCESS OK is placed into the control panel's event log. Reports in the event log that were not sent before the Reset Panel are never sent to the D6500 or D6600.

When RPS programming changes parameters, a Parameters Changed Report is sent to the D6500 or D6600. If any programming changes are made, perform a Reset-bye.

When RPS contacts the control panel, the RPS passcode and DataLock code are verified. If the control panel's passcode matches and the DataLock code does not, the control panel still generates a RPS Access OK Event; however, the session ends immediately.

To prevent the control panel from answering the telephone automatically, enter Blank in the **Answer Armed** and **Answer Disarmed** prompts in this section.

2.7.2 Log Threshold Reports

If communication with RPS is unsuccessful, or if no phone number is programmed in **RPS Ph**, the control panel generates Log Threshold and Bad Call to Ram. This indicates the log is filling and the control panel cannot download its events.

If there is no **RPS Ph** programmed, the control panel generates the Log Threshold and Bad Call to RPS Events immediately. Bad Call to RPS Events are logged only locally. If an **RPS Ph** is programmed, the control panel makes multiple attempts to reach RPS before sending the reports. Refer to the **RPS Ph** prompt in *Section 2.7.3 RPS Callback Reports* for an explanation of dialing characteristics.

2.7.3 RPS Callback Reports

When dialing the RPS phone number, the control panel makes two attempts to reach RPS. If the control panel does not reach RPS on the first two attempts, it waits 10 min then tries six more times with a 10-min interval between each attempt. One hour after the last failed attempt, the control panel starts dialing the RPS phone number again. It makes two more attempts then waits 10 min and tries six more times with 10-min intervals between each attempt before generating a Bad Call to RPS Report and abandoning the effort.

Remote Program Dialing Exception: When an RPS phone number is programmed, the user can call RPS by entering [COMMAND][4][3] and pressing the [NEXT] key until CALLRPS? is displayed. Press [ENTER]. Only one attempt is made to contact RPS.

RPS Passcode

Default: 999999

Selection: 0 to 9, A to F
(six characters required)

Enter six characters. Do not use a space in the passcode.

The control panel verifies the remote programming software at the central station has valid access before connecting using the RPS passcode.

Log % Full

Default: Blank

Selection: 1 to 99, or Blank

This parameter determines how full the memory log can be before initiating a call to RPS at the central station. This allows the central station to call the control panel and copy the memory log before messages are overwritten.

Blank disables the Log Threshold and Log Overflow Events. These events are not entered in the log or reported to the D6500 or D6600 or the local printer.

The control panel continues to log events after the Log Threshold Report is sent. When it reaches 100% capacity (memory logger is full and previously stored events are overwritten), the control panel generates a local Log Overflow Event.

The control panel does not call RPS again until it downloads the log and the Log % Full percentage is reached. These events are also sent to the control panel's event log and to the local printer(s) if installed.



The Log Overflow Event is not sent to the central station unless **Expanded Test Rpt** is programmed **Yes**.



Failure to program the RPS telephone number results in a BAD CALL TO RPS trouble event sent to the central station when the log threshold is reached. Refer to the **RPS Ph** prompt on page 34 for information about programming the RPS telephone number.

RPS Call Back

Default: No	
Selection: Yes or No	
Yes	When the control panel hears the correct RPS passcode, it hangs up the phone, seizes the phone line, then dials the programmed RPS phone number (refer to the RPS Ph prompt on page 34). This ensures that the control panel only communicates with RPS units connected to the programmed phone number. If the call is answered manually, the call back must be initiated manually.
No	The RPS session starts immediately. No call back is required. The control panel can engage in RPS sessions when called from any phone number and a proper RPS passcode is identified.

This function allows the control panel, after it verifies the RPS passcode, to provide an additional level of security by hanging up and dialing the RPS phone number at the central station before allowing any upload or download.



When using the RPS Call Back feature, be sure to program the character “C” as the last digit in the RPS phone number when using **DTMF Dialing**.

RPS Line Monitor

Default: Yes	
Selection: Yes or No	
Yes	Allows the control panel to communicate with RPS after the answering machine answers the phone.
No	Use No if the control panel does not share the phone line with an answering machine.

This program item enables a control panel that shares a phone line with an answering machine to communicate with RPS at the central station, even though the answering machine answers the phone. You must program **Answer Armed** or **Answer Disarmed**. The control panel must be in the correct armed state.



Program this item **No** if it causes false seizures of the phone line or if you do not use RPS. This indicates that a device using the same frequency tone is also using the phone line to which the control panel is connected.



If **RPS Call Back** is programmed **Yes**, the control panel hangs up the phone after the RPS tone and a proper RPS passcode is identified. It then calls the RPS phone number.

Answer Armed

Default: Refer to the program record sheet	
Selection: 1 to 15, or Blank	
Blank	No answer.
1 to 15	The control panel answers the phone after the specified number of rings when all areas are master armed.

Set the telephone ring counter to answer when all areas are master armed. If any area in the control panel is perimeter armed or disarmed, the Answer Disarmed ring counter is used.



The remote programming software (RPS) considers perimeter armed as a disarmed state.

Answer Disarmed

Default: Refer to the program record sheet	
Selection: 1 to 15, or Blank	
Blank	No answer.
1 to 15	The control panel answers the phone after the specified number of rings when any area in the system is in a perimeter armed or disarmed state.

Set telephone ring counter to answer when any area is in a perimeter armed or disarmed state.



The RPS considers perimeter armed as a disarmed state.

RPS Ph

Default: Blank	
Selection: Blank or up to 24 characters	
Blank	Control panel does not dial a phone number for RPS.

1 to 24
charactersEnter up to 24 characters to define
dialing characteristics.

This is the phone number the control panel dials to contact RPS. The control panel dials the programmed number on **Phone #5 (RPS Ph #)** when any of the following events occur:

- Log % Full threshold is achieved.



If **Log % Full** is programmed with a value (1 to 99) and an RPS phone number is programmed, the control panel dials the RPS phone number when the log threshold is reached. This function is not available in RPS. Do not program **Log % Full** and an RPS phone number at the same time.

- The control panel is contacted by RPS and RPS Call Back is programmed **Yes**.
- The user enters COMMAND 43 and selects the call RPS option from the menu. On the D1255:
 - Press [COMAND][4][3].
 - Press [NEXT] until CONTACT RPS? appears, then press [ENTER].
 - Wait for RPS VIA PHONE? to appear, then press [ENTER].



The control panel tries to contact RPS only once using this method.

Refer to *Section 6.4 SDI RPS Parameters* on page 126 for other connection methods.



Refer to *Phone 1* in *Section 2.1 Phone* on page 11 for descriptions of special programming values for the RPS Phone number.

2.8 Miscellaneous

Duress Type

Default: 0

Selection: 0, 1, 2, or 3

0	Do not send a duress event with any passcode.
1	<p>Increase the last digit by 1 to generate an alarm. For example, if the passcode is 6123, 6124 activates a duress alarm.</p> <p>If the last digit of the passcode is 0, a duress alarm occurs when the user enters 1 as the last digit of the passcode.</p> <p>If the last digit of the passcode is 9, a duress alarm occurs when the user enters 0 as the last digit of the passcode.</p>
2	<p>Increase the last digit by 2 to generate an alarm. For example, if the passcode is 6123, 6125 activates a duress alarm.</p> <p>If the last digit of the passcode is 8, a duress alarm occurs when the user enters 0 as the last digit of the passcode.</p> <p>If the last digit of the passcode is 9, a duress alarm occurs when the user enters 1 as the last digit of the passcode.</p>
3	Send a Duress event when any Passcode with L# Send Duress set to Yes is entered.

This program item determines if users add one (+1) or two (+2) to the last digit of the passcode. To activate a duress alarm, the user increases the value of the last digit of the passcode when entering it at the keypad.



Duress is enabled in Area Parameters by setting **A# Duress Enable** to **Yes**.



The duress alarm activates when a user enters the duress passcode followed by the termination keys ([ESC] or [ENT]).

For SIA CP-01 Compliance

Duress Type must be set to 3.

Cancel Report

Default:	No
Selection:	Yes or No
Yes	Send Cancel and Fire Cancel Reports according to routing.
No	Do not send Cancel and Fire Cancel Reports.

A Cancel and Fire Cancel Report is created when a passcode is entered to silence an Alarm Bell or a Fire Bell before the bell time expires.

For SIA CP-01 Compliance

This prompt must be set to **Yes**.

2.9 Area Parameters

This programming module contains three programming categories: Area Parameters, Bell Parameters, and Open/Close Options.

2.9.1 Area Parameters**Area**

Default:	1
Selection:	1 to 8

Enter the area number you are programming.

A# Area On

Default:	Yes (Area 1 only)
Selection:	Yes or No
Yes	Enable area.
No	Disable area.

Use this program item to enable or disable the area specified.



Area 1 must be enabled:

- System events such as power and phone supervision do not send a report correctly if Area 1 is disabled.
- When programmed **No**, points assigned to this area do not generate events, show at the keypad when arming and disarming, or send status reports. All user authority in this area is turned off while the area is disabled.



To meet UL 864 requirements, set **A# Area On** to **Yes**.

A# Acct Number

Default:	0000
Selection:	For Modem and Contact ID (four-digit account numbers): 0000 to 9999, BBBB to FFFF
	For Modem (ten-digit account numbers): 0000000000 to 9999999999, BBBB BBBB BB to FFFFFFFF

Determines the account number for this area. An account number must be assigned to each active area.

Account numbers are used to group areas together. Each area can have a different account number, or several areas can share the same account number. The control panel uses the account number as a reference for arming and keypad text displays.

Contact ID: Only the last four digits are sent.

Modem IIIa²: Enter a four-digit or ten-digit number.

2.9.2 Programming Account Numbers in 9000 Series Control Panels

The GV2MAIN handler can program a four-digit or ten-digit account number for each area.

Programming Four-Digit Account Numbers

To program a four-digit account number (such as 1234) using the D5200 Programmer, you must enter leading 0s (zeroes) for Digits 1 to 6, then enter 1234 into Digits 7 to 10. When 0s are entered for the first six digits (Digits 1 to 6), the 9000 Series Control Panel treats this as a four-digit account number. Refer to *Table 23*.

Table 23: Programming Four-Digit Account Numbers

D5200 Programmer		
A# Acct#	Dgt 1&2	0 0
A# Acct#	Dgt 3&4	0 0
A# Acct#	Dgt 5&6	0 0
A# Acct#	Dgt 7&8	1 2
A# Acct#	Dgt 9&10	3 4

The D5200 account number entry shown in *Table 23* appears in RPS as 1234.



Although the D5200 allows the character “A” to be entered into the account, do **not** use this character for the account number.

Any account number digits containing “A” for digits 1 to 6 that were uploaded to and received by RPS are **not** displayed.

If an “A” is sent erroneously to the control panel from the D5200 for any of Digits 1 to 6, correct this by:

- Entering six leading 0s from the D5200 and sending them to the control panel,
or
- Entering six leading 0s from RPS, followed by the four-digit account number, and sending them to the control panel.

Programming Ten-Digit Account Numbers

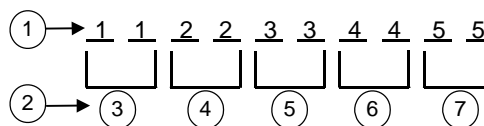
To program a ten-digit account number (such as 1122334455) using the D5200 Programmer, you must enter a character for each of the ten digits. Refer to *Table 24*:

Table 24: Programming Ten Digit Account Numbers

D5200 Programmer	
A# Acct# Dgt 1&2	1 1
A# Acct# Dgt 3&4	2 2
A# Acct# Dgt 5&6	3 3
A# Acct# Dgt 7&8	4 4
A# Acct# Dgt 9&10	5 5

The D5200 account number entry shown in *Table 24* appears in RPS as shown in *Figure 2*.

Figure 2: Account Number Entry



- 1 - RPS account number entry
- 2 - Corresponding D5200 account number digits
- 3 - Digits 1 and 2
- 4 - Digits 3 and 4
- 5 - Digits 5 and 6
- 6 - Digits 7 and 8
- 7 - Digits 9 and 10



Although the D5200 allows the character “A” to be entered into the account, do **not** use this character for the account number.

A# FA Bypass Max

Default: 1

Selection: 0 to 99

Specify the maximum number of combined Controlled points that can be faulted or bypassed when arming this area.

Refer to the prompts **P## FA Retrnable** and **P## BA Retrnable** in *Section 4.2 Point Responses* on page 91 for returning a point to the system when the point returns to normal or when the area is disarmed.



Users can bypass more points than the number entered here during the disarmed state. It is only when the user attempts to Bypass Arm an area (or areas) that this restriction is enforced.

A# Delay Res

Default: No

Selection: Yes or No

Yes	Point Restoral Report is not sent until the bell time expires or user acknowledges alarm condition.
No	Restoral Reports are sent when point restores, regardless of bell time.

A# Exit Tone**Default:** Yes**Selection:** Yes or No

Sounds an exit tone during exit delay at all keypads assigned to this area.



You can turn off exit tones for individual keypads by programming the appropriate **CC# 1 to 8** as **No** in **CC# Exit Tone**.

A# Exit Dly Time**Default:** 60**Selection:** Blank (0) to 600 (in 5 sec increments)

Exit delay time for this area when Master Exit or Perimeter Exit arming.



Points programmed for instant alarm response generate alarms immediately, even during exit delay. To avoid instant alarms on points adjacent to the perimeter when leaving the area, program **P## Type** as 3 (Interior Follower).

For SIA CP-01 Compliance

The Exit Delay Time must be between 45 sec and 255 sec.

A# Auto Watch**Default:** No**Selection:** Yes or No

Yes	When the area is disarmed, Watch Mode turns on automatically.
No	When the area is disarmed, Watch Mode must be turned on or off manually.



Controlled points must be programmed as **P## Watch Point** to generate a watch tone.

A# Verify Time**Default:** 60**Selection:** 10 to 60 (in 1-sec increments)

Use alarm verification with smoke detectors to reduce the number of false fire alarms. When Verify Time is programmed, the control panel can check smoke detector point activations before generating alarm signals.



- **Do not** enable the Cross Point feature in point indexes designated for Fire points.
- Check with your authority having jurisdiction (AHJ) to determine the maximum verification time allowed.

Points are programmed individually to activate the verification feature. Refer to *Section 4.1 Point Index* on page 87. Any resettable Fire point can activate alarm verification for the area to which it is assigned. Use separate area alarm-verification relays.

To enable alarm verification on a point, program **Point Index**, Fire Point, Alarm Verify, and Resettable as **Yes**.

When an Alarm Verification point senses an alarm, the control panel automatically removes power to all Resettable points connected to the area's Reset Sensors relay. The sensor reset removes power to the sensors for the amount of time programmed in Verify Time. When power is reapplied, a 60-sec confirmation window begins. If the detector is still in alarm and experiences another alarm during the confirmation window, or a different Resettable Verification point in the area senses an alarm, an alarm occurs.

Example: Verify Time is set for 20 sec. The alarm verification cycle starts when the detector senses smoke or fire. No report occurs.


When the detector senses smoke or fire, the area's sensor reset relay interrupts power to points connected to it for the time in Verify Time.

When power restores to the points, the 60-sec confirmation window starts. If any detector, reset during the verification time, experiences another alarm during the confirmation window, an alarm occurs. If no activity occurs during this period, no alarm occurs and the verification window ends. If a Verification point senses another alarm after the window ends, a new verification cycle begins. Refer to *Table 25* on page 39 for an example of **Verify Time**.



To meet UL 864 requirements, set **A# Verify Time** to 60 sec.

Table 25: Verify Time

	Verification Point Activation	Verify Time/Reset Sensors	60 sec Confirmation	Restart Alarm Verification Cycle if an Alarm Verification point activates.
Example: Total Cycle time 80 sec		20 sec	60 sec	

A# Duress Enable

Default:	No
Selection:	Yes or No
Yes	Enable Duress alarm for this area.
No	Disable Duress alarm for this area.

Refer to **Duress Type** in Section 2.8 Miscellaneous on page 35 for an explanation of duress.







The passcode you normally use for duress is not valid in an area with **A# Duress Enable** set to **No**.

If a passcode with the appropriate **L# Disarm** authority is used to duress disarm an area with A# Duress Enable set to **No**, NO AUTHORITY appears in the display. Also, if the keypad display is moved to an area with **A# Duress Enable** set to **No** using [COMMAND][5][0], a valid duress disarm passcode does not send a duress report.

For SIA CP-01 Compliance:

A# Duress Enable must be set to **Yes**.

A# Area Type

Default: Regular Selection: Regular, Master, Associate, or Shared	
Regular	Arms or disarms as an independent area.
Master	<p>Does not allow arming for this area unless all associate areas with the same A# account number are master exit delay armed or master armed. CHK AREA displays if the associate areas are not armed. Exception: RPS allows master areas to be armed without all associate areas being in the armed state.</p> <p>A master area can be disarmed regardless of the armed state of the other areas in the account.</p> <p>Multiple master areas can be programmed in a single account.</p> <div>  <p>CC# Scope affects master arming.</p> <p>Area: When arming a master area that has CC# Scope set to Area for all keypads, all associate areas within the same account must first be armed independently by other means.</p> <p>Panel Wide or Account Wide: When arming a master area from a keypad with CC# Scope set to Panel Wide or Account Wide, all associate areas enters exit delay as soon as the master area is armed. If there is a shared area within the same account, it begins its exit delay after all associate areas are armed.</p> </div> <div>  <p>Using the arming sked (S## Function 1) requires that you first use an arming sked to arm the associate areas before using an arming sked to arm the master area. Arming master areas with RPS, Keyswitch, or Auto Close parameters (refer to <i>Section 2.9.5 Open/Close Options</i> on page 43) occurs before all associate areas are armed</p> </div>
Associate	<p>Allows arming and disarming regardless of the armed state of the other areas with the same A# account number. Use this area type with a master area and associate it by using the same account number.</p> <div>  <p>Keypads assigned to associate areas, when used with shared areas, must have CC# Scope programmed.</p> </div>
Shared	<p>Shared areas cannot be armed using a passcode, key switch, token or card, sked, or RPS.</p> <div>  <p>Arming commands intended for a shared area must be executed on a keypad with Panel Wide scope by a user with appropriate authority in all areas. Shared areas associate with all Associate areas regardless of their account assignments.</p> </div>

2.9.3 Shared-Area Characteristics

Arming a Shared Area

A shared area arms automatically when all associate areas are armed. As soon as the last associate area is armed, the shared area automatically begins its arming sequence. Passcode, key switch, sub-controls, or RPS cannot arm shared areas. To display faulted points at associate areas, the shared and associate areas must have the same account number.

Disarming a Shared Area

Shared areas automatically disarm when any associate area in the control panel is disarmed. Passcode, tokens, cards, key switch, sub-controls, or RPS cannot disarm shared areas.

Shared Area Arming Sequence

When shared areas automatically begin to arm, the arming is based on the **A# Exit Dly Time** is based on the A# Exit Dly Time of the Shared Area.

Shared Area Not Ready

If a point is faulted in the shared area, CHK AREA appears on the associate keypad that is arming the last associate area. Associate area keypads can show faults from shared areas as long as the shared areas fall within the scope of the associate area.

Force Arming a Shared Area

When CHK AREA appears, press [ESC] to show FORCE ARM at the associate keypad. Pressing [ENTER] force arms the shared area if:

- the user has authority to bypass points,
- the point is bypassable, and
- the number of faulted points does not exceed the force arm maximum amount for the shared area.



Remember to include the shared area in the associate area's scope.

Viewing Shared Area Armed Status

View Area Status can be used from a keypad outside of the shared area to view the shared area's armed state.

Silencing Sounders in the Shared Area

Silence shared area alarms and troubles from any keypad.

To silence sounders, the user needs an authority level assigned to the shared area. If the user also has the authority to arm or disarm the area, then ALREADY ARMED or ALREADY DISARMED momentarily appears.

Access Control Readers Assigned to the Shared Area

The shared area momentarily disarms then begins the exit delay sequence, allowing a user to walk to an associate area and disarm. If the token or card reader assigned to the shared area includes any associate area in the **D## CC# Scope** (in the access handler), both the associate area and shared area disarms when the token or card is presented.

Closing Reports for Shared Areas

If Closing Reports for shared areas are needed, assign passcodes a valid authority level in the shared area.

2.9.4 Bell Parameters

The D9412GV3 and the D7412GV3 have two main types of annunciation: Fire Bell and Burg Bell. Both Fire and Burg Bells share the same terminal (Terminal 6) on the control panel as shipped from the factory.

If a simultaneous Fire Bell and Burg Bell occur, the Fire Bell takes precedence over the Burg Bell regardless of which relay or terminal output they share.

When the Fire and Burg Bells share the same output and a Fire Bell occurs while the Burg Bell is ringing, the Fire Bell pattern overrides the Burg Bell pattern. At the end of the fire time, the burg pattern resumes.

When the Fire and Burg Bells share the same output and a Burg Bell occurs while a Fire Bell sounds, the control panel waits until the Fire time expires before starting the Burg Bell.

Either a single bell (panel-wide) or a number of bells (area-wide) can be used on the control panel. For programming these applications, refer to *Section 2.13.1 Area Relays* on page 79.

When both Fire and Burg Bells occur simultaneously and a user enters a valid passcode, a Fire Cancel Report for the fire alarm and a Cancel Report for the burg alarm is sent to the central station if Cancel Reports is programmed **Yes**.

Area**Default:** 1**Selection:** 1 to 8

Enter the area number you are programming.

A# Fire Time**Default:** 6 min**Selection:** 1 min to 90 min

Enter the number of minutes the bell rings for Fire Alarm points. The relay activated for this time is programmed in **A# Fire Bell** in Area Relays.

The bell output begins as soon as the fire alarm occurs. It shuts off the bell when the programmed number of minutes expires.

If programmed for 1 min, the output can be anywhere from 0 to 60 sec of bell time. Program Fire Time for 2 min or more to ensure you have ample output time.



To meet UL 864 requirements, program **A# Fire Time** for at least 5 min. Check with your AHJ to determine the appropriate bell time for your geographical area.

A# Fire Pat**Default:** Pulse**Selection:** Steady, Pulse, CaStd, TmCod3

Steady Steady Output

Pulse Pulse March Time
120 beats per minute, at an even tempo

CaStd California Standard
10 sec On + 5 sec Off + 10 sec On + 5 sec Off. This sequence repeats until bell time expires.

TmCod3 Temporal Code 3
0.5 sec On, 0.5 sec Off, 0.5 sec On, 0.5 sec Off, 0.5 sec On, 1.5 sec Off; pattern repeats. This sequence repeats for a minimum of 3 min and with a $\pm 10\%$ tolerance.

Select the bell pattern this area uses to signal an alarm on a Fire point.

Press the [Space] bar to scroll through the selections. Press [Enter] when the correct selection appears in the display.



When an alarm occurs on two Fire points sharing the same relay, the bell pattern of the most recent fire event takes precedence.

A# Burg Time**Default:** 6 min**Selection:** 1 to 90 min (in one-minute increments)

4 min for UL
5 min for ULC

Enter the number of minutes the bell rings for Burglary Alarm points. The relay activated for this time is programmed in **A# Alarm Bell** in Area Relays.

The bell output begins as soon as the burglary alarm occurs. It shuts off the bell when the programmed number of minutes expires.

When the control panel's internal clock begins a new minute, it considers the first minute expired. Program **Burg Time** for 2 min or more.



Check with your AHJ to determine the appropriate bell time for your geographical area.

For SIA CP-01 Compliance:

A# Burg Time must be 6 min or more.

A# Burg Pat**Default:** Steady**Selection:** Steady, Pulse, CaStd, TmCod3

Select the bell pattern this area uses to signal an alarm on a Non-fire point.

Press the [SPACE] bar to scroll through the selections. Press [ENTER] when the correct selection appears in the display.

A# Single Ring

Default:	No
Selection:	Yes or No
Yes	One bell output per arming period. After one alarm, alarms on any Non-fire points in the same area cannot restart the bell until the armed state changes. An alarm on a different point in same area restarts bell output.
No	Restart bell output with each alarm event.

Determines if an alarm from a non-fire point can restart the alarm bell time with each Alarm Event, or only start alarm output once per arming period.

This does not silence the keypad alarm bell tone, or prevent any reports. This feature does not affect Fire points. Fire points restart bell time with each new alarm.



If an alarm occurs on a 24-hour point while the area is disarmed, arming that area with a key switch does not clear the A# Single Ring flag.



Silencing the bell resets **A# Single Ring**.

A# Bell Test

Default:	No
Selection:	Yes or No
Yes	Start Bell Test.
No	Do not start Bell Test.

Provides alarm output from the relay programmed at **A# Alarm Bell** after the Closing Report is confirmed or the exit delay time expires.

Bell Test After Confirmation

In areas that send Opening and Closing Reports, the Bell Test occurs after the control panel sends the Closing Report and receives an acknowledgment from the central station receiver. For proper operation of the Bell Test after closing confirmation, the following rules apply:

- The control panel must send Opening and Closing Reports to the central station.
- Do not use restricted openings and closings or Opening and Closing Windows.

Area Armed Confirmation

In areas that do **not** report opening and closing activity, the alarm bell relay output for this area activates for 2 sec after exit time expires.



Multiple Bell Tests occur: When more than one area is armed at the same time (such as using the ARM ALL AREAS? function), the bell rings for 2 sec with a 2 sec pause between each bell activation if all areas have the same exit delay time programmed. Otherwise, the Bell Test occurs as each area arms and it completes its exit delay time.

When areas arm simultaneously and report to the central station, the Bell Test occurs as the central station receiver confirms each area.

2.9.5 Open/Close Options

Programming determines if Opening, All Normal Closing, and Force Arm/Bypass Closing Events are sent to the remote central station. Without remote reports, all control panel and area arming (Closing Events) and disarming (Opening Events) default to local events.

Use this programming category to determine which opening and closing supervision characteristics are needed.

There are three ways to generate reports from the control panel. You can generate reports by account, by area, or a combination of both.



Opening and Closing Events are sent only by users with the proper authority settings.

To suppress reports:

- Use Opening/Closing Windows to suppress reports for a specified period of time and then automatically turn them on again.
- Use the Restricted O/C options. A Closing Report is sent if the user is force arming, sending duress, or bypass arming. An Opening Report is sent if the user is disarming during an alarm condition or unbypasses points when disarming. If the system is normal, no Opening or Closing Report is sent.



For the scheduled suppression of Opening and Closing Reports, refer to *Section 5.1.1 Opening and Closing* to define Opening and Closing Windows.

Account Opening and Closing Reports

Opening and Closing Reports are sent by account when the last area in a group of areas with the same account number(s) is armed.

Area Opening and Closing Reports

Closing Reports are sent for each area as it is armed. The account number is also sent for each area.

Customizing Account Opening and Closing Reports

You can eliminate area Opening and Closing Reports from selected areas in the account by programming **A# Area O/C** as **No** for those areas.

Combination Account and Area Opening and Closing Reports

To send both account openings and closings, and individual area openings and closings for all areas in the account, you must:

- Program **A# Acct O/C** as **Yes** for all areas in the account.
- Program **A# Area O/C** as **Yes** for all areas in the account.

Closing Reports: When areas in the account are independently armed, each area generates an Area Closing Report. When the last area is armed, it also generates an Account Closing Report.

Opening Reports: When the first area in the account is disarmed, it generates an Account Opening Report along with an Area Opening Report. When the remaining areas in the account are disarmed, each area generates an Area Opening Report.

Area Only Opening Closing Supervision Features

Use these features to supervise opening and closing activity by area. Auto Close, Fail To Open, and Fail To Close all work independently of the **A# Acct O/C** feature. To use these features, program O/C Windows.

Area

Default: 1

Selection: 1 to 8

Enter the area number you are programming.

A# Acct O/C

Default: No

Selection: Yes or No

Yes

Send Opening and Closing Reports by account.

Use this selection if the control panel sends reports to an automation system that cannot interpret multiple Area Opening and Closing Reports.

An Account Opening Report is generated when the first area in an account is opened (disarmed). After the Account Opening Report is sent, disarming other areas in the account does not generate another Account Opening Report. An Account Closing Report is generated only when the last area in an account is closed (armed). Opening and Closing Reports for accounts do not contain any area information.

Opening and Closing Windows affect Account Opening and Closing Reports: If an account opening or closing is generated while an Opening or Closing Window for this area is in effect, and **Disable O/C** in Window is programmed **Yes**, the report is not sent. Use the same opening and closing window times for all areas sharing the same account number.

No

Do not send Opening and Closing Reports by account.

Determines if this area generates Account Opening and Closing Reports. Program this item the same for all areas in the account.

A# Area O/C**Default:** Yes**Selection:** Yes or No

Yes	Include the Area # and generate Opening and Closing Reports for this area when it is armed.
No	Do not include the Area # or generate Opening and Closing Reports for this area.

Determines if the area number and the account number are reported at arming and disarming. As long as **Account O/C** is **No**, the account number sends a report when arming this area individually. If **Account O/C** is **Yes**, all areas with the same account number must also be armed.

An Area Opening Report is generated when each area is opened (disarmed). An Area Closing Report is generated when each individual area is closed (armed).



Do not program this item as **Yes** if the control panel reports to an automation system that cannot interpret multiple Area Opening and Closing Reports.

A# Disable O/C in Window**Default:** Yes**Selection:** Yes or No

Yes	<p>Do not send Opening and Closing Reports to the central station if they occur inside an active window.</p> <p>If an Opening or Closing Report occurs outside a window, send it with an early or late modifier. Refer to <i>Section 5.1.1 Opening and Closing</i> on page 105.</p> <p>The active window must be a Closing Window for Closing Reports. It must be an Opening Window for Opening Reports.</p>
No	<p>Send Opening and Closing Reports to the central station even when they occur inside a programmed window. If an opening or closing occurs outside of the appropriate window, it reports but does not have an early or late modifier.</p> <p>If you want to monitor all opening and closing activity and use features provided by Opening and Closing Windows, program this item as No, and program the appropriate O/C Windows.</p>

Determines if opening and closing activity is reported when it occurs inside an Opening or Closing Window, as programmed in O/C Windows.

Reports are always logged and printed on a local printer, if installed.

A# Auto Close**Default:** No**Selection:** Yes or No

Yes	<p>The area automatically master arms at the end of the Close Window.</p> <p>When the area is armed automatically, a Closing Report is sent if the Area or Account Reports are programmed to do so.</p>
No	Do not automatically arm the area at the end of the Close Window.

With this program item, the control panel can automatically master arm the area at the end of the Closing Window regardless of the previous armed state.



When an area master arms automatically at the end of a Close window, the system disregards the settings in **A# Force Arm Max** and **P## Bypassable** for any faulted points. The faulted points arm when they return to normal state.

A# Fail to Open**Default:** No**Selection:** Yes or No

Yes	Fail to Open Report is sent for this area if the area was not disarmed when the Opening Window stop time occurred.
No	Fail to Open Report is not sent for this area.

Use to determine if a Fail to Open Report is sent for this area. This can determine if a user failed to disarm the area before the Opening Window expiring. Normal Opening and Closing Reports do not need to be programmed to use this feature.

A# Fail to Close

Default: No	
Selection: Yes or No	
Yes	Fail to Close Report is sent for this area if the area is not armed when the Closing Window stop time occurs. Note: Program an exit delay time in Exit Dly Time .
No	Fail to Close Report is not sent for this area. <ul style="list-style-type: none"> If Auto Close is programmed Yes, a Fail to Close Report is sent because it occurs when the Closing Window stop time occurred. If Disable O/C in Window is Yes, the Fail to Close Report is followed by Closing Late or Force) Close Late.

This item determines if a Fail to Close Report is sent for this area. Use to determine if a user failed to arm the area before the Closing Window expires. Normal Opening and Closing Reports do not need to be programmed to use this feature.

A# Restrictd O/C

Default: No	
Selection: Yes or No	
Yes	Restrict Opening and Closing Reports for this area. A# Area O/C must be programmed Yes to generate Restricted Opening and Closing Reports. Note: If a passcode is not required for arming or disarming and this item is Yes , the area sends only Restricted Opening and Closing Reports. In this case, Restricted Reports are sent without User ID. Opening/Closing Window does not affect this report. Windows do not prevent sending Restricted Opening and Closing Reports from being sent. Early or late designations are not added to Opening or Closing Reports when they are sent according to the rules for Restricted Opening or Closing Reports.
No	Do not Restrict Opening and Closing Reports for this area. Regardless of programming in Authority Levels L## Restricted O/C , reports are not restricted in this area when this item is programmed as No . Note: Was Force Armed and Forced Close Events can still be sent to the central station if enabled in Routing when force arming the system.

This item determines if this area can restrict Opening and Closing Report activity.

A Restricted Opening Report refers to the control panel sending an Area Opening Report only when the area is disarmed after a non-fire alarm.

A Restricted Closing Report refers to the control panel sending a Force Closed Report only when the area was master armed with Controlled points that were faulted during the arming sequence. The sequence of reports generated by a restricted closing is: Was Force Armed, Forced Point, and Force Closed.

A# Perimeter O/C**Default:** No**Selection:** Yes or No

Yes	This area can send Perimeter Opening and Closing Reports.
No	This area cannot send Perimeter Opening and Closing Reports.

This item determines if this area can send Perimeter Instant and Perimeter Delay Closing Reports and normal Opening Reports to the central station. Opening and Closing Windows do not suppress this event. Refer to the **L## Perimeter O/C** prompt on page 75.



This reporting requires modem format reporting. Some central station automation systems cannot process these reports.

A# Latest Close Time**Default:** 00:00**Selection:** 00:00 to 24:00

Use to set a Latest Close Time boundary value for this area. If the Latest Close Time value is non-zero, the time of day specified with the Extend Close feature cannot be greater than or equal to this value. A zero value for **A# Latest Close Time** disables the feature for the area.

Example: If A# Latest Close Time is set for 17:30, the user can extend the close time to as late as 17:29.

This prompt is used only when an O/C Window is assigned to an area. Make entries in 30-min increments using a 24-hour format. Use times that begin on the hour or the half-hour only. For example, enter 2:30 PM as 14:30. Enter 1:00 AM as 01:00. To set the Latest Close Time for midnight, use a value of 24:00. The latest close time allowed by the Extend Close feature is 24:58, because of internal limitations in the control panel.



The default entry of 00:00 **disables** the Latest Close Time feature for this area.

The control panel sets all windows for the next day when the control panel clock turns to midnight. The control panel must cross the midnight boundary before any changes in that default setting occur.

To extend across midnight, **you must use two windows:**

- To suppress reports before midnight, use one window (for example, 20:00 start to 23:59 stop).
- To suppress reports immediately after midnight, use another window (for example, 00:01 start to 02:00 stop).

2.9.6 Arming Features**A# Two Man Rule****Default:** No**Selection:** Yes or No

Yes	Two valid unique passcodes are required to disarm the area.
No	A single passcode with a valid authority level can disarm the area.



The D720 Keypad does not support the Two-Man Rule feature.

Use this parameter when disarming an area that is Master Armed. After recognizing the first valid passcode, the system requests a second passcode to disarm the area. If the entry delay expires before the entry of a second valid **unique** passcode, an alarm condition occurs. This function works only when you use Passcode Disarm.



When you are disarming an area with **A# Two Man Rule** set to **Yes**, the keypad waits for the time equal to the **A# Exit Delay Time**. If the second passcode is not entered before the prompt times out, the rule resets and waits for the first passcode again.



If the area is already in an alarm condition, the first valid passcode entered after the alarm occurs silences the bell but **does not disarm** the area. Enter Code 2 appears on the display. A second valid **unique** passcode is necessary to disarm the area.



This feature is not allowed for use with SIA CP-01 compliant installations. Consult the local authority having jurisdiction (AHJ) for proper usage. Refer to your control panel's program entry guide for programming information.

Parameter Setup Requirement:

Two Man Rule can be completed only by entering two valid unique passcodes with **L## Passcode Disarm** authority.



To avoid unintended results for the end user of the system:

- Set **CC# Scope** to **Area Wide** for keypads assigned to areas with the Two Man Rule feature.
- Avoid setting the **A# Two Man Rule** to **Yes** in an area where **A# Early Ambush** is set to **Yes**.



Use this feature in banks or other facilities that might require a higher level of security to gain access to a vault or other protected area.

D1255 Keypad

After the first valid passcode is entered, the D1255 replaces the scrolling DISARM NOW and the Point Text display with the SECOND CODE:.display

When the user presses the first digit of the second code, the display changes to SECOND CODE: *.

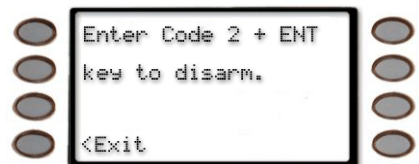
SECOND CODE: appears for 19 sec. If no digits are pressed, the display returns to normal and the area does not disarm. If a second code is entered, the area disarms and an Opening report is sent with the User ID of the first user. If the second code entered is the same as the first code, is invalid, or does not have **L## Disarm** authority, the keypad shows NO AUTHORITY and returns to idle text or entry delay.

D1260 Keypad

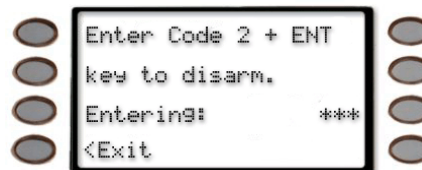
In the D1260, after the first valid passcode is entered, the following message appears for 3 sec.



Then the next message appears requesting a second code.



When the first digit of the second code is pressed, the following message appears. As each digit is pressed, an additional asterisk appears.

**A# Early Ambush**

Default:	No
Selection:	Yes or No
Yes	Two valid passcodes are required to disarm the area within the time period specified in Early Ambush Timer. The second valid disarm passcode must be entered within a time limit. Refer to Early Ambush Timer on page 140. If the second passcode is not entered within the time limit, the system generates a Duress Event based upon the primary user.
No	A single passcode with a valid authority level can disarm the area.

The **Early Ambush** disarming feature is intended for use when you disarm an area that is in the Master Armed state, but it can also be used with the Perimeter and Instant Armed states. After the first valid passcode is entered, the area is disarmed and the keypad displays the disarmed idle text normally. This function operates only when you use Passcode Disarm.

If the second valid disarm passcode is entered, the D1255 Keypad shows CODE 2 VALIDATE and sounds the Watch Mode tone. Only the Watch Mode tone appears on the D720 Keypad.

The D1260 Keypad sounds the Watch Mode tone and the following text appears.



Parameter Setup Requirement:

The Early Ambush timer can be started and stopped only by passcodes with the L## Passcode Disarm authority.



To avoid unintended results for the end user of the system:

- When a keypad is assigned to an area that has the Early Ambush feature enabled, set the **CC# Scope** value to Area Wide.
- If an area has **A# Two Man Rule** set to **Yes**, do not set **A# Early Ambush** to **Yes**.

During an alarm, after the first passcode is entered, the Early Ambush timer still begins. A Cancel Report might be generated, depending upon the bell time, and the keypad displays Alarm Silenced normally. If the second valid disarm passcode is entered, the keypads indicate that the second passcode is valid. Refer to the **Secondary Ambush Code** prompt on page 140 for information about the unique behavior of the two passcodes.

For SIA CP-01 Compliance:

This feature is not allowed for use with SIA CP-01 compliant installations.

A# Exit Restart

Default: Yes	
Selection: Yes or No	
Yes	Delay armed points in this area restart the exit delay timer if violated during the exit delay time.
No	Delay armed points continue to count down normally if violated during the exit delay time.



This feature must be disabled for UL Line Security/Encryption applications.

When enabled, this feature activates when a controlled point with delay alarm response changes from normal to faulted and back to normal during the exit delay. When activated, if any controlled point in the same area with delay alarm response is faulted, the exit delay time restarts. The exit delay continues until it expires or the area changes arming states. This operation can occur only once in an arming cycle.



To avoid the possibility of false alarms in Associate areas, do not use the **A# Exit Restart** feature in areas with **A# Area Type** set to **Shared**.

For SIA CP-01 Compliance

This prompt can be set to **Yes** or **No**.

A# Arm No Exit

Default: Yes	
Selection: Yes or No	
Yes	Switch the arming state to Perimeter if no Perimeter Delay point faults occurred.
No	Keep the area in Master Arm if no Perimeter Delay point faults occurred.

This parameter switches the arming state of an area from Master Armed to Perimeter Armed if no perimeter points with delay response were activated during the exit delay time. Only the final armed state is reported and displayed at the keypads.



The A# Arm No Exit feature does not operate in areas with **A# Area Type** set to **Shared**.

For SIA CP-01 Compliance:

A# Exit Restart can be set to **Yes** or **No**.

A# Exit Warning

Default: Yes	
Selection: Yes or No	
Yes	Pulse the alarm output for the last 10 sec of the Exit Delay time.
No	Do not pulse the Alarm Bell output during the Exit Delay time.

When enabled, the Alarm Bell output pulses on and off every 2 sec for the remaining 10 sec of the Exit Delay time.

For SIA CP-01 Compliance

A# Exit Warning must be set to **Yes**.

A# Entry Warning

Default: Yes	
Selection: Yes or No	
Yes	Pulse the alarm output for the last 10 sec of the Entry Delay time.

No	Do not pulse the Alarm Bell output during the Entry Delay time.
----	---

When enabled, the Alarm Bell output pulses on and off every 2 sec for the remaining 10 sec of the Entry Delay time.

For SIA CP-01 Compliance

A# Entry Warning must be set to **Yes**.

2.10 Keypad (Command Center)

This programming module contains three programming categories: Cmd Cntr Assignment, Area Text, and Custom Function.

2.10.1 Keypad (Command Center) Assignment

This programming category assigns a keypad to an area and determines if the keypad is supervised. The keypads are connected to the control panel using a two-wire serial data interface (SDI) bus.

This bus can support up to eight supervised keypads, each with its own unique keypad address (CC) and corresponding DIP switch address settings. If the keypads are not supervised, you can install multiple keypads with the same DIP switch address setting for up to 32 unsupervised keypads.

Cmd Center

Default: 1							
Selection: 1 to 8							
SDI CC#	Address Number	DIP Switch Setting					
		1	2	3	4	5	6
1	1	ON	ON	ON	ON	--	ON
2	2	OFF	ON	ON	ON	--	ON
3	3	ON	OFF	ON	ON	--	ON
4	4	OFF	OFF	ON	ON	--	ON
5	5	ON	ON	OFF	ON	--	ON
6	6	OFF	ON	OFF	ON	--	ON
7	7	ON	OFF	OFF	ON	--	ON
8	8	OFF	OFF	OFF	ON	--	ON


Enter the keypad (CC) number for the SDI address you are programming. This number corresponds to the DIP switch address settings shown.


Switch 5: On=Encoding Tone On (default), Off=Encoding Tone Off


CC# Supervised**Default:** Refer to the program record sheet**Selection:** Yes or No


Yes	Only one keypad can be installed for this CC SDI address.
No	More than one keypad can be installed using this CC SDI address with the same address DIP switch setting.

Supervise this SDI address and generate Trouble SDI Reports and local trouble annunciation if a problem occurs with this keypad or the SDI bus.

	To meet UL 864 requirements, set CC# Supervised to Yes for the fire annunciation keypad.
---	--

	Keypads that share the same address setting display the same text and emit the same tones, regardless of which keypad's keys are pressed. Trouble SDI # Reports are always reported as Area 1, Account 1 Events regardless of the area the SDI device is assigned.
---	---

	When this prompt is Yes , you cannot have duplicate DIP switch settings.
---	---

	When a D1260 Alpha V Keypad is assigned to a keypad address, you must program CC# Enhanced Command Center as Yes .
---	--

CC# Area Assign**Default:** 1**Selection:** 1 to 8

Blank is not a valid entry.

Enter the area number where you are installing this keypad or keypads with this address and the same DIP switch settings.


CC# Scope**Default:** Refer to the program record sheet**Selection:** Panel Wide, Custom, No Keypad, Area, and Account


Panel Wide	A panel-wide keypad can view information and perform Arming and
------------	---

	Disarming functions for all areas in the control panel. A panel-wide keypad can cross account boundaries. This is normally used with a master area.
Account	An Account keypad can view information, and perform Arming and Disarming functions for all areas with the same A# Acct Number , in Area Parameters. This is normally used for an associate area.
Area	An area keypad is restricted to viewing information and Arming or Disarming functions for the area to which it is assigned.
Custom	A custom keypad shows information and allows arming and disarming for specific areas you select.
No Keypad	No keypad installed at this address. CALL FOR SERVICE display shows, indicating the control panel is not polling this address.

This program item is used to define the areas affected when an arming command is executed on this keypad, the areas this keypad can view, and the areas to which this keypad can move.

Press the [SPACE] bar to scroll through the selections. Press [ENTER] when the correct selection appears in the display.

	In applications where keypads include more than one area, active alarms in remote areas must be acknowledged before arming or disarming the local area.
---	---

	The following prompt is visible only when you program CC## Scope to Custom. If you change the keypad scope selection to Custom from Panel Wide, Account, or Area, the settings from the previous CC# Scope selection become the default settings for the custom parameters in CC# A1 [through A8] in Scope . Before exiting from a custom program, check each area and ensure that it is enabled and disabled correctly.
---	--

CC# A1 [through A8] in Scope**Default:** Refer to the preceding important note**Selection:** Yes or No

Yes	Include this area in the scope of this keypad.
-----	--

No	Do not include this area in the scope of this keypad.
----	---

Determines whether any of the eight areas (Area 1 to Area 8) and Doors (Door 1 to Door 8) are included in the scope of this keypad for viewing status, arming or disarming, and controlling doors from the keypad.

CC# Entr Key Rly

Default:	Blank
Selection:	1 to 128, A, B, C, and Blank
Blank	The [ENTER] key is not used to activate a relay.
1 to 128, A, B, C	Assign the relay number that activates when [ENTER] is pressed at this keypad after the user enters a valid passcode.

Enter Key Relay: Program the relay number that activates momentarily for 10 sec when a user enters a valid passcode and presses the [ENTER] key on the keypad. Two events are generated when this function is used: RELAY ### SET with User ID, and RELAY ### RESET without User ID. The system logs this action as two events.

- Entering a valid code and pressing [ENTER] silences a ringing bell.
- Using **CC# Entr Key Rly** for a low-level access control strike on a door does not shunt a point.



When programmed to activate a relay, the [ENTER] key cannot be used for any other function.

Relays used for this function must not be shared with any other point, sensor reset, control panel, or bell functions. Sharing can cause errors in relay operation.

CC# Entr Cycl Dr

Default:	No
Selection:	Yes or No
Yes	The [ENTER] key is used to cycle the door programmed for CC Assign Door.
No	The [ENTER] key is not used to cycle the door.

Enter Key Cycle Door: Program this prompt as **Yes** to start the door cycle sequence for the door number programmed in **CC# Assign Door** when a user enters a valid passcode and presses [ENTER]. This includes shunting the point assigned to the door. ACCESS GRANTED prints on the local printer and at the central station receiver, if programmed.



- The service passcode cannot be used for the **CC# Entr Cycl Dr** application.
- When programmed to activate a relay, the [ENTER] key cannot be used for any other function.
- Relays used for this function must not be shared with any other point, sensor reset, control panel, or bell functions. Sharing can cause errors in relay operation.
- The door does not cycle if **Entr Key Rly** is programmed.
- 9210 NOT READY appears at this keypad when you press [ENTER] if the D9210B is not programmed with a **D# Entry Area** (in the RADAXS handler) or if CC Assign Door does not have a door number assigned.



- If a door is not programmed for this prompt and a door is not assigned to the area using the **D# Entry Area** in the RADAXS handler, 9210 NOT READY appears at this keypad when you attempt to add a user. The message indicates that the control panel cannot start the Add User Mode until a door is assigned to this keypad.
- Assigning a door to a keypad is not necessary for the user to control the door(s) using the Door Control function. Any door that is active can be controlled by a user who has the appropriate door control authority. The door control functions are available to a valid user at any keypad with access to the area where the door is assigned.

CC# Assign Door

Default: Blank

Selection: 1 to 8, Blank

Blank	No door controller is assigned for adding tokens.
1 to 8	The door controller assigned to this keypad is used to read new tokens when the Add User Mode is initiated.

If the assigned door remains open and this keypad has the **CC# Close Door Warning Tone** set to **Yes**, the CLOSE DOOR # message appears on this keypad.



During the Add User Mode, tokens or cards, door control requests, and RTE/REX do not function. Put the Door Mode into an **unlocked** state before adding users if there is heavy activity for this door.

CC# Trouble Tone

Default: Yes

Selection: Yes or No

Yes	Panel-wide trouble tones sound and visual displays show at this keypad.
No	Panel-wide troubles do not sound. Visual displays still show.

Determines whether this keypad, or any keypad with the same address setting, emits the panel-wide trouble tones (power, phone, SDI bus, and Zonex bus).



To meet UL 864 requirements, set **CC# Trouble Tone** to **Yes**.



Panel-wide trouble tones do not include Point Troubles, Buzz on Fault, or Close Door Now.



Assign two CCs to the same area so one keypad emits the tone and another does not.

CC# Entry Tone

Default:	Yes
Selection:	Yes or No
Yes	This keypad sounds entry tones.
No	This keypad does not sound entry tones.

Determines whether this keypad, or any keypad with the same address setting, emits the entry delay tone. Any Delay point within the area scope of this keypad starts the entry sequence.



This prompt allows you to manage the tone by keypad. Entry Tone can also be turned off when programming your **P## Entry Tone** off in **Point Index**.



Assign two CCs to the same area so one keypad emits the tone and another does not.

For SIA CP-01 Compliance

CC# Entry Tone can be set to **Yes** or **No**.

CC# Exit Tone

Default:	Yes
Selection:	Yes or No
Yes	This keypad sounds exit tones.
No	This keypad does not sound exit tones.

Determines whether this keypad, or any keypad with the same address setting, emits the exit delay tone during the delay arming of an area(s). Any keypad with a scope to arm this area can initiate the exit tone sequence.

This prompt allows you to manage the tone by keypad. Exit Tone can also be turned off when programming **A# Exit Tone** in Area Parameters.

The cadence and pitch of the exit tone increase for the last 10 sec of the exit delay time.



This SIA CP-01 required feature is not supported on the D720 and D720B Keypads.



Assign two CCs to the same area so one keypad emits the tone and another does not. Set one keypad for CC EXIT TONE = YES, and one to EXIT TONE = NO.

For SIA CP-01 Compliance

CC# Exit Tone can be set to **Yes** or **No**.

CC# Arm Now Warn

Default:	No
Selection:	Yes or No
Yes	This keypad activates a tone and displays PLEASE CLOSE NOW.
No	This keypad does not activate the tone or display PLEASE CLOSE NOW.

Determines whether this keypad sounds a tone and displays the PLEASE CLOSE NOW warning on the keypad when a Closing Window activates, indicating the area automatically arms soon.

CC# Close Door

Default:	No
Selection:	Yes or No
Yes	This keypad sounds a tone and displays CLOSE DOOR #.
No	This keypad does not sound the tone or activate the display.

Determines whether this keypad sounds an audible tone and displays the CLOSE DOOR # warning on the keypad. This occurs when the door is physically held open past the shunt time and the extend time has a value greater than zero for the door assigned to this area in **CC# Assign Door**. Refer to the *D9210B Program Entry Guide* (P/N: 32207).

CC# EnhancCmdCtr

Default:	No
Selection:	Yes or No
Yes	This keypad is a D1260 Alpha V Keypad.
No	This keypad is not a D1260 Alpha V Keypad.

When a D1260 Alpha V Keypad is installed at this keypad address, this item must be set to **Yes**.



Reboot the system to enable an Alpha V keypad.

To reboot the system, close and open the reset switch, labeled "S1 RESET," located in the upper right corner of the control panel.

CC# Passcode Follows Scope

Default: Yes	
Selection: Yes or No	
Yes	<p>Master Arming allows a user to change the armed state of the areas within the scope of this keypad. If the areas in the scope are already at the intended armed state, they remain in that state.</p> <ul style="list-style-type: none"> If the area to which this keypad is assigned is armed, entering a valid passcode disarms this area and all other areas assigned to the scope of this keypad. If the area to which this keypad is assigned is disarmed, entering a valid passcode arms this area and all other areas assigned to the scope of this keypad.
No	<p>Restricts the scope of the keypad to the Area programmed in CC# Area Assign for the purpose of executing L## Passcode Arm and L## Passcode Disarm only.</p>

Use this program to determine if this keypad follows **CC# Scope** or if it only arms or disarms the area to which it is assigned. The user must have authority enabled in **L## Passcode Arm** and **L## Passcode Disarm**. This feature does not affect the Function List arming and disarming commands.



Tokens and cards disarm according to this prompt. If this prompt is **No**, tokens disarm only the Area to which the CC# is assigned. The user must have disarming rights for tokens and cards programmed at the **Disarm Level**. The user does not need disarming and arming authority for the keypad.



You can use this prompt for a group of account-wide keypads that only arm the area to which they are assigned, even if the user has a passcode with arming authority rights in all areas.

CC# Scroll Lock

Default: No	
Selection: Yes or No	
Yes	Prevents the idle system status text from scrolling automatically. Requires user intervention to advance.
No	Allows the idle system status text to scroll automatically without user intervention

Use this parameter to enable a special non-scrolling option for the idle system status display text on a keypad. This keypad mode requires the user to press the PREV or NEXT key on the keypad to unlock the display and begin scrolling through the system status displays.

CC# Menu Key Lock

Default: No	
Selection: Yes or No	
Yes	If set to Yes , the user is prompted to enter a passcode after pressing the Menu key on the keypad. The items programmed in the Menu List for this specific keypad are filtered by the user's authority level. Only those items in the menu list for which the user has authority appear.
No	If set to No , when the user presses the Menu key, all items that are programmed in the Menu List for the Command Center Address (Keypad Address) appear, regardless of the user's authority level.

Determines if the Menu Key, when pressed, requires a passcode to access the functions.



If this parameter is set to **Yes**, users must enter a passcode after pressing the Menu

key. When the passcode is validated, only those functions for which the user has authority appear in the list. If a function in the Menu List is passcode protected (refer to Keypad Functions in *Section 2.11.2 User Interface* on page) the user does not need to enter the passcode again.

CC# Abort Display

Default: Yes	
Selection: Yes or No	
Yes	This keypad shows the Alarm Aborted message for all aborted alarms within its scope.
No	This keypad does not show the Alarm Aborted message for all aborted alarms within its scope.

This parameter enables or disables the ALARM NOT SENT message when an alarm is aborted before transmission occurs.

For SIA CP-01 Compliance

CC# Abort Display can be set to **Yes** or **No**.

CC# Cancel Display

Default: Yes	
Selection: Yes or No	
Yes	This keypad shows the Cancel Report Sent message for all canceled alarms within its scope.
No	This keypad does not show the Cancel Report Sent message for all canceled alarms within its scope.

This parameter enables or disables the CANCEL RPT SENT display message when an alarm is canceled after transmission occurs. To show this message, Cancel Report must be set to Yes. Refer to **Cancel Report** on page 36.

For SIA CP-01 Compliance

CC# Cancel Display can be set to **Yes** or **No**.

2.10.2 Area Text

Use this programming category to create custom Idle Text displays for the keypads.



Each display can be programmed with up to sixteen alphanumeric characters, including: A to Z, 0 to 9, ?, &, @, -, *, +, \$, #, _, /.

Characters not listed are invalid and cannot be used for text.

Area

Default: 1
Selection: 1 to 8

Enter the area number you are programming.

Area# Is On

Default: Refer to the program record sheet
Selection: Sixteen alphanumeric characters

Enter the text for this area that appears when the area is master armed or master instant armed and other areas sharing the same account number are not yet master armed. This display does not appear when the area is perimeter armed.

Area# Not Ready

Default: Refer to the program record sheet
Selection: Sixteen alphanumeric characters

Enter the text for this area that displays when the area is disarmed but points are faulted.

Area# Is Off

Default: Refer to the program record sheet
Selection: Sixteen alphanumeric characters

Enter the text for this area that displays when the area is disarmed and no points are faulted.

Area# Acct Is On

Default: Refer to the program record sheet
Selection: Sixteen alphanumeric characters

Enter the text that appears when all areas sharing the same account number are master armed. The ACCT IS ON text appears at all keypads assigned to these areas, if more than one area has the same account number. The ACCT IS ON text also appears if only one area in the system is used. Refer to the prompts **CC# Area Assign** and **Area # Acct Is On** in *Section 2.10.1 Keypad (Command Center) Assignment* on page 50. When all areas in the account are master armed, the Area # Is On text is replaced by the ACCT IS ON text if the area is armed before all other areas with the same account number.

Blank Entry

A blank entry disables the ACCT IS ON display for this area. An account wide area shows the AREA # IS ON text instead of the ACCT IS ON text.

Unique ACCT IS ON Text

Each area can have unique ACCT IS ON text, or you can program the same text in each area of the account so when all the areas in the account are armed, they all show the same text.

D1260 Alpha V Keypad

Although it is not programmed in this area, the D1260 Alpha V Keypad can display up to sixteen characters for an Area Name on line 1 of its display. The Area Text (**Area # Is Off**, **Area # Not Ready**, **Area # Is On**, and **Acct # Is On**) programmed in this module appears on line 2 of the D1260 Alpha V Keypad. When programming custom text, it should be logical to users viewing it on the D1260. For example, the Area Name Text can be programmed to display Front Office and the **Area # Is Off** text (programmed in this section) could be programmed to display Ready To Arm. The D1260 would then show on line 1 Front Office and on line 2, Ready To Arm.

2.10.3 Custom Function

Use custom functions to simplify complex keystroke sequences entered at the keypad. These items are similar to speed dialing on a telephone. When the custom function appears on the keypad, a user can execute a request by pressing [ENTER]. You can have up to sixteen custom functions and restrict their use by area and authority level.

Each **Custom Function ###** item has sixteen characters of programmable text (**CF### Text**). When the Custom Function is assigned to the menu **M## Function** (refer to *Section 2.12 Function List* on page 77) the user can press [PREV] or [NEXT] to scroll to **CF### Text**. The user accesses the menu by pressing [MENU] on the keypad.

The user needs the appropriate authority level enabled for the **L## C Function 128 to 143** in *Section 2.11 User Interface* on page 60, to use the custom function.

Consider the scope of the keypad used to access the Custom Function. Each Custom Function is enabled in the function menu by **M## CC Address 1 [through 8]** (refer to **M## CC Address 1 [through 8]** on page 78). If the Custom Function is not assigned to a specific keypad address, it does not appear in the menu.

Custom Function

Default: 128

Selection: 128 to 143

Enter the Custom Function number you want to program. You can program up to sixteen Custom Functions, which are numbered 128 to 143.

CF### Text

Default: Refer to the program record sheet

Selection: Sixteen alphanumeric characters.
See *Section 2.10.2 Area Text* on page 56 for valid character entries.

Determines the menu text displayed at the keypad for the custom function item. Use this text to represent the functions performed by this menu item.

CF### Key Strokes**Table 26: CF### Key Strokes**

Default:	Refer to the program record sheet		
Selection :	Up to 32 characters: 0 to 9, A, B, C, D, E		
Selection	D1255 Key	D1255 Faceplate Label	D1260 Key
0 to 9	0 to 9		0 to 9
A	[COMMAND]		[COMMAND]
B	[PREV] (previous)		NA
C	[ESC] (escape)	MENU	NA
D	[NEXT]		NA
E	[ENT] {enter}	YES	[#ENTER]
C1*	NA		(softkey 1)
C2*	NA		(softkey 2)
C3*	NA		(softkey 3)
C4*	NA		(softkey 4)
C5*	NA		(softkey 5)
C6*	NA		(softkey 6)
C7*	NA		(softkey 7)
C8*	NA		(softkey 8)

* Softkey selections are stored as two keystrokes.

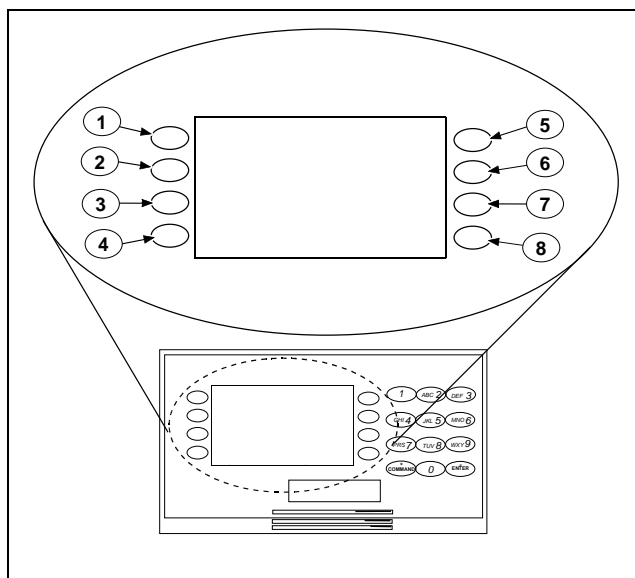
The keystrokes simulate any sequence of keystrokes the user can perform at a keypad. You can program up to 32 keystrokes for each Custom Function.

D5200 Data Entry

Use the [↓] key on the D5200 to move the cursor to the first data entry line. To enter more than sixteen keystrokes, you must fill the first line of the data entry line before you move to the second line. If you make entries on the second line, and the first line has less than sixteen characters, the second line clears when you press [ENTER].



The scope of the keypad where you access the Function List can affect the way the Custom Function operates.



- | | |
|--------------------|--------------------|
| 1 - Softkey 1 (C1) | 5 - Softkey 5 (C5) |
| 2 - Softkey 2 (C2) | 6 - Softkey 6 (C6) |
| 3 - Softkey 3 (C3) | 7 - Softkey 7 (C7) |
| 4 - Softkey 4 (C4) | 8 - Softkey 8 (C8) |

Figure 3: Softkey Locations on the D1260 Keypad

Programming Custom Function Keystrokes

- Find the command you want to execute in the *User Interface* section of the program record sheet. Single digit commands must be programmed with 9 as the second digit.

Table 27: CF### Custom Function Keystrokes

Command	Keystroke
1 (Master arm area)	A19
2 (Perimeter instant arm)	A29
3 (Perimeter delay arm)	A39
6 (Watch Mode)	A69
7 (Special alert)	A79
8 (Perimeter partial arm)	A89
9 (Special alert)	A99
0 (Bypass a point)	A09

- When **CF### Custom Function** is programmed with **P**, the corresponding custom function number is passcode protected. The **CF### Custom Function** prompt is under GV2MAIN > User Interface > Cmd Center Functions. The passcode protected custom function can be added to a keypad's function list by programming its number in the GV2MAIN > Function List > M# Function prompt.
- 128 to 143 Enable Custom Function 128 through 143 (Menu Function only):** This function determines if a passcode is needed to access a Custom Function from the menu list. ENTER PASSCODE (or Enter Passcode + Enter Key on the D1260) appears when this function is passcode protected.



If a command within the Custom Function is passcode protected, ENTER PASSCODE appears at the keypad. The user must enter a valid passcode before proceeding with the rest of the Custom Function. If a passcode is not entered within 10 sec, the Custom Function times out and the display returns to idle text.



Skeds cannot execute Custom Functions that are passcode protected. The D720 LED keypad does not support Custom Functions that are passcode protected.

Some functions cannot be entered directly because they are nested inside a higher-level function. To automatically execute these functions, you must add the appropriate keystrokes.

- For example: The Change Display (COMMAND 49) function has three sub-functions: Bright Display, Dim Display, and Date/Time Display.
 - To turn up the display, enter:
[A][4][9][E]
 - To dim the display, enter:
[A][4][9][D][E]
 - To display time and date, enter:
[A][4][9][B][E]
- Custom Functions can perform several tasks at one time. For example:
 - To toggle relays 7, 8, and 9 in one Custom Function enter:
[A] [5] [4] [7] [E] [E] [8] [E] [E] [9] [E] [E] [C]
 - To add a temporary passcode, enter:
[A] [5] [6] [3] [0] [E] [E] [9] [8] [7] [E] [E] [D] [E] [1] [E] [1] [E] [1] [E] [1] [E] [1] [E] [1] [E] [1] [E] [1] [E] [C]
This adds user 30, passcode 987 with authority level 1 in all areas.
 - To delete the passcode, enter:
[A] [5] [3] [3] [0] [E] [E] [E] [C]

To program multiple-area Arming or Disarming functions, use keystroke sequences including COMMAND 50 (Move to Area) and COMMAND 1.



Custom function cannot be used to change time (such as Daylight Saving Time). Use **Skeds S## Function Codes 13 and 14** to adjust for Daylight Saving Time (refer to **S## Custom Function** prompt in *Section 5.2 Skeds* on page 114.

Example 1

Execute the third function in a keypad menu function list:

```
D1255 CDDE
D1260 C8C7C5
```



The custom functions in Example 1 **are not** compatible between keypad types.

Example 2

Instant master Arm (CMD 11):

```
D1255 A11
D1260 A11
```



The custom functions in Example 2 **are** compatible between keypad types.



The GV3 control panel series uses separate keystrokes to program the custom functions that accurately represent the two separate user interfaces, the D1255 and D1260 keypads.

Custom functions written for the D1255 that use the [PREV], [ESC], and [NEXT] keys do not work on the D1260.

Custom function written for the D1260 that use the softkeys (located on the sides of the keypad display) do not work when executed from the D1255 keypad.

2.11 User Interface

Define which functions can be used by each of the fourteen user authority levels. Each user can be assigned the same or different authority level by area. The user has rights in the area where the keypad is assigned, based on the authority level assigned to the user's passcode for that area.

When the passcode is entered at the keypad, the control panel checks the authority level. The control panel executes the function only in areas where the passcode has the authority to use the function.

2.11.1 Commands

Similar to command initiation used in other Bosch Security Systems, Inc. products, the Commands method provides continuity in the arming commands across product lines and makes an easy transition for dealers using other Bosch Security Systems, Inc. products. With commands, the end user presses [COMMAND] and then the numeral of the command to initiate. For example, [COMMAND][2] arms the perimeter of the area. Some prompts can be accessed only from a menu. These prompts are indicated by (Menu Function only). To access these functions, press [MENU], enter the function number, and use the [PREV] and [NEXT] keys to scroll through the choices.

The *D9412GV3/D7412GV3 Program Record Sheet* (P/N: F01U143072) lists the commands available with the system. Command numbers are shown in the column labeled Command. If a particular function does not have a command number, it can be accessed only through the Function List.

If you plan to use only commands to operate the system, and to arm and disarm by entering a passcode, you do not need to program Custom Function or Function List.

2.11.2 Keypad Selections

Programming choices in this section determine if keypad functions are disabled (blank), enabled (E), or passcode (P) restricted.

Press the [SPACE] bar to scroll through the selections. Press [ENTER] when the correct selection appears in the display.

Table 28: Keypad Programming Choices

Selection	Description
Blank	Disable the function panel-wide. The keypad shows NO AUTHORITY if you access the function using a command or the Function List.
E	Enable the function panel-wide. The function can be executed without entering a passcode.
P	Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level. Refer to <i>Section 2.11.4 Authority Level Selections</i> on page 67.



Refer to *Section 2.11.4 Authority Level Selections* on page 67 for a detailed description of the functions on the following pages. These parameters determine only if the authority level functions are passcode protected.

Master Arm Delay

Default:	P
Selection:	Blank, E, or P
P	Passcode: Required for all users with Master Arm Delay enabled for their authority level.
E	Enable: A user does not need a passcode to use [COMMAND][1].
Blank	Disable Master Arm Delay cannot be accessed in the function menu or started with a command even if this function is enabled for the user's authority level.

Function No.	Function Name	Alternate Keystroke
2	Master Arm Delay	[COMMAND][1]


Use this arming function to master arm disarmed areas. If enabled, the following arming choices are available to the user with this authority.

Mstr Arm Inst

Default: Blank		
Selection: Blank, E, or P		
Function No.	Function Name	Alternate Keystroke
3	Master Arm Instant	[COMMAND][1][1]

Use this arming function to master arm instant areas that are disarmed. Entry and exit delays are **not** provided with this arming function. This causes a Perimeter and Interior Delay point to act as an Instant point.

For SIA CP-01 Compliance


	This feature is not allowed to be used with SIA CP-01 compliant installations.
---	--

Perim Instant

Default: P		
Selection: Blank, E, or P		
Function No.	Function Name	Alternate Keystroke
4	Perimeter Instant Arm	[COMMAND][2]

Instant arms all perimeter points with point response that starts an instant alarm (refer to **P## Pt Response** in Section 4.2 Point Responses on page 91) in the area where the keypad is assigned. Entry and exit delays are **not** provided with this arming function. This function causes a Perimeter Delay point to act as a Perimeter Instant point.

For SIA CP-01 Compliance

	This feature is not allowed in SIA CP-01 compliant installations.
---	---

Perim Delay

Default: P		
Selection: Blank, E, or P		
Function No.	Function Name	Alternate Keystroke
5	Perimeter Delay Arm	[COMMAND][3]

Delay arms all Perimeter points in the area where the keypad is assigned. Entry and exit delays are provided with this Arming function. This function does not cause a Perimeter Instant point to act as a Delay point.

Watch Mode

Default:	E
Selection:	Blank, E, or P

Function No.	Function Name	Alternate Keystroke
6	Watch Mode	[COMMAND][6]

This function informs you when a perimeter point or interior point that is programmed as **P## Watch Point** is faulted while the area is disarmed. Interior points do not emit a Watch Tone if the area is perimeter armed. This function provides keypad audible or visual and optional relay activation (refer to **A # Watch Mode** in Section 2.13.1 Area Relays on page 79).

Perim Partial**Default:** P**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
7	Perimeter Partial Arm	[COMMAND][8]

Use this function to arm normal perimeter points and force-bypass faulted perimeter points, regardless of their P## Bypassable setting. When these force-bypassed perimeter points return to normal, they automatically return to service, even if P## FA Returnable is set to No.

Perimeter Partial arming has entry and exit delays.



Perim Partial ignores the **A# FA Bypass Max** entry in *Section 2.9 Area Parameters* on page 36.



Local Only Reporting: No Closing Report is sent to the central station, but a Perimeter Delay Closing Event is generated in the event log.

View Area Stat**Default:** P**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
8	View Area Status	(Menu function only)

Use this function to view the armed status of all areas within the scope of the keypad assigned to this area. The armed states include A# AREA # IS OFF (disarmed), A# AREA # IS ON (master delay armed), ALL ON INSTANT (master instant armed), and AREA # PERIM ON (perimeter instant armed or perimeter delay armed). All area types, master, associate, regular, and shared can be viewed using this function.

View Memory**Default:** E**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
9	View Event Memory	[COMMAND][4][0]

Use this function to view prior alarm, trouble, and supervisory activity occurring since the last time the system armed. Event memory is not cleared until the area re-arms.

View Pt Status**Default:** E**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
10	View Point Status	(Menu function only)

Use this function to view points assigned to the area where the keypad is assigned. This function shows point text and the electrical condition (normal, open, short, and missing) of each point in the area.

Walk Test**Default:** E**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
11	Walk Test	[COMMAND][4][4]

Use this function to test Controlled points in areas within the keypad's scope without sending reports to the central station. 24-hour points cannot be tested using this Walk Test Mode.

.Fire Test**Default:** P**Selection:** Blank, E, or P

Function No.	Function Name	Alternate Keystroke
12	Fire Test	[COMMAND][5][8]

Use this function to test 24-hour points in areas within the scope of the keypad where the function is entered. Controlled points, **P## Type 1, 2, 3**, cannot be tested using the Fire Walk Test Mode.

Send Report

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
13	Send Report	[COMMAND][4][1] or [COMMAND][4][2]

Use this function to test the communication link between the control panel and the central station receiver(s). It can send a Test Report or a Status Report to the phone numbers programmed in Routing. The Test Report includes additional information if **Expand Test Rpt** is enabled in *Section 2.1 Phone* on page 11.

2.11.3 Access Control Functions**Door Control**

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
14	Door Control	[COMMAND][4][6]

#14 Door Control [COMMAND][4][6]

This top level display must be enabled for the user to access the cycle door, unlock door, and secure door functions (refer to *Section 2.11.4 Authority Level Selections* on page 67). Use this item when programming door control in your function menu.

Access Ctl Level

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
37	Access Control Levels	(Menu function only)

Shows the current on or off state of control levels 1 through 14, pertaining to Access Control Only, (**L## Access Level** and **L## Disarm Level**). The user can toggle levels on and off and invalidate access control levels during an extended period. This change only affects the user's token or cards; it does not affect keypad Door Control functions.

Chg Display

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
15	Change Display	[COMMAND][4][9]

Use this function to select either a bright or dim display with loud or soft keypad warning tones. You can also choose the time and date display.

Chg Time/Date

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
16	Change Time and Date	[COMMAND][4][5]

Use this function to set the time and date in the control panel.

Chg Passcode

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
17	Change Passcodes	[COMMAND][5][5]

Use this function to change your passcode. This is a panel-wide function that can be executed from any keypad assigned to an area where the user has authority.



Refer to *Section 2.11.4 Authority Level Selections* on page 67 for a detailed description of the functions on the following pages. These parameters determine only if the authority level functions are passcode protected.



Regardless of whether an E or a P is entered when a COMMAND 55 is performed, the keypad asks for the user's current passcode first.

Add User

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
18	Add User	[COMMAND][5][6]

Use this function to add or change passcodes, add or change tokens or cards and Sub-users, and add or change control panel authority levels (L##) by area.

Del User

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
19	Delete User	[COMMAND][5][3]

Use this function to delete a user's passcode and tokens or cards. It does not delete user names.



This function deletes the passcode, master user, and all sub-users associated with the user number.

Extend Close

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
20	Extend Close	[COMMAND][5][1]

Use this function to change the expected closing time for the area. The window cannot be adjusted until the Close Early Begin time passes and the Closing Window is active.

View Log

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
21	View Log	(Menu function only)

Use this function to view all of the system events, their time stamps, User IDs, or point numbers. User Name and Point Text are **not stored** in the event log, but they appear when the control panel matches them with the User ID ### and the Point ###.

Each event appears on one line in the log. Any information related to that event appears on a separate line in the log.

Because events in the log are not uniform in length, the control panel can store from 500 to 1000 events.

Print Log

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
22	Print Event Log	(Menu function only)

Use this function to print all the events stored in the control panel beginning at the start date and ending with the last event in the log.

User Cmd 7

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
23	User COMMAND 7	[COMMAND][7]

Use this function to activate an alarm programmed in COMMAND 7 in the RADXPNTS Handler.

User Cmd 9

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
24	User COMMAND 9	[COMMAND][9]

Use this function to activate an alarm programmed in COMMAND 9 in the RADXPNTS Handler.

Bypass a Pt

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
25	Bypass a Point	[COMMAND][0]

Use this function to bypass individual points that have **P## Bypassable** enabled. Points within the scope of the keypad can be bypassed where the function is entered (refer to *Section 2.10.1 Keypad (Command Center) Assignment*) on page 50.

The control panel ignores alarms and troubles, and does not display point faults when a point is bypassed.

Unbypass a Pt

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
26	Unbypass a Point	[COMMAND][0][0]

Use this function to unbypass individual points that are programmed either **P## FA Retrnable** or **P## Bypass Returnable**. Points within the scope of the keypad can be unbypassed where the function is entered (refer to *Section 2.10.1 Keypad (Command Center) Assignment*) on page 50. The control panel responds to alarms and troubles, and displays point faults when a point is unbypassed.

Reset Sensors

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
27	Reset Sensors	[COMMAND][4][7]

Use this function to activate the Reset Sensors function for Fire or Intrusion points programmed as **P## Resettable** in *Section 4.1 Point Index* on page 100. Points within the scope of the keypad where the function is entered reset. Refer to *Section 2.10.1 Keypad (Command Center) Assignment* on page 50.

Change Relay

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
28	Change Relays	[COMMAND][5][4]

Use this function to manually set and reset Relays 1 through 128 (1 through 64 in a D7412GV3) that are installed in the system.

Remote Program

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
29	Remote Programming	[COMMAND][4][3]

Use this function to start remote programming software (RPS) sessions. When the phone is ringing at the control panel, starting this function causes the control panel to seize the line.

Move to Area

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
30	Move to Area	[COMMAND][5][0]

Use this function to switch the keypad's assignment temporarily to a different area. This command can be used to perform any function that can be performed by a keypad assigned to the area in programming.

Users are limited to performing functions enabled by the authority level they have in the area to which the keypad is moved. After 15 sec of no activity at the keypad, the keypad reverts back to the originally programmed area.

Display Rev

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
32	Display Software Revision	[COMMAND][5][9]

Use this function to show the control panel's software revision number in the keypad display.

Service Walk

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
33	Service Walk Test	(Menu function only)

Use this function to Walk Test all 246 points in the entire control panel regardless of the **P## Type**.



The Service Walk Test is available on the D9412GV3 using the Service Menu [9][9][ENT]. The D7412GV3 **does not** include the Service Walk Test in the Service Menu. In the D7412GV3, the Service Walk Test function must be enabled in the Function List to access the Service Walk Test.

Default Text

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
34	Default Text	[COMMAND][5][7]

Determining the armed state of an area using the programmed custom text might be difficult. Use this function to switch temporarily to the control panel default text, shown on the program record sheet.

Change Skeds

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
35	Change Skeds	[COMMAND][5][2]

Execute this panel-wide function from any keypad assigned to an area where the user has authority. Use this function to change the **S## Time** from the keypad to make adjustments to Skeds.

Invisible Walk Test

Default: P
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
36	Invisible Walk Test	(Menu function only)

This function allows a user with the **L## Invisible Walk Test** authority to test invisible interior or perimeter controlled points that are within the scope of the keypad, without sending reports to the central station. Invisible points must have the **P## Invisible Pt** function programmed **Yes**.

Custom Functions

C Function 128 [through 143]

Default: E
Selection: Blank, E, or P

Function No.	Function Name	Alternate Keystroke
128 through 143	Enable Custom Functions 128 through 143	(Menu function only)

When enabled, Custom Function determines if a passcode is required when accessing a custom function from the menu list. ENTER PASSCODE (or Enter Passcode + Enter Key on the D1260) appears when this function is passcode protected. If a command within the Custom Function is passcode protected, the keypad displays ENTER PASSCODE (or Enter Passcode + Enter Key on the D1260) and waits for the user to enter a valid passcode before proceeding with the rest of the Custom Function. If a passcode is not entered within 10 sec, the Custom Function times out and the display returns to idle text.

2.11.4 Authority Level Selections

Use *Section 2.11.4 Authority Level Selections* on page 67 to determine which Authority Level can access keypad functions that are passcode protected. Selecting **Enable items** in the Authority Level section is not necessary if the keypad function is disabled or enabled. Each individual function has two selections you can use for the authority level you are programming.

Press the [SPACE] bar to scroll through the selections. Press [ENTER] when the correct selection appears in the display.

Table 29: Authority Level Selections

Authority Level	Description
Blank	Disabled: This function is not authorized for the user who is assigned this authority level.
E	Enabled: This function is authorized for the user who is assigned this authority level.

Authority Level

Default: 1
Selection: 1 to 14

Enter the number of the authority level you want to program. Authority Level 15 (Service Passcode) cannot be edited.



To determine the **L##** default values on pages 67 through 76, refer to the *User Interface* section for the GV2MAIN Handler in the program record sheet.

L## Disarm

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name
1	Disarm

Use the disarming function to disarm areas that are master armed or perimeter armed. If enabled, the following disarming choices are available to the user with this authority:

- **DISARM ALL:** Disarms all areas within the **CC# Scope** of the keypad being used by accessing the Function Menu and the authority level of the user performing the function.
- **DISARM AREA:** Disarms only the displayed area.



Many options are available for arming and disarming. Selecting an option depends on **A# Area Type** and **CC# Scope**. Read the definitions of area type in *Section 2.9 Area Parameters* on page 4 and **CC# Scope** in *Section 2.10.1 Keypad (Command Center) Assignment* on page 50.

L## Master Arm Delay

Default: Refer to the program record sheet
Selection: Blank or E
:

Function No.	Function Name	Alternate Keystroke
2	Master Arm Delay	[COMMAND][1]

Master arms areas based on the **CC# Scope** of the keypad using an exit delay time.

When this item is accessed through the Function List, Master Arm All allows the user to arm all areas according to the authority level of the user and within the **CC# Scope** of the keypad using an exit delay time.

Arm Area arms only the area displayed. If COMMAND 1 is used, it arms only the area where the keypad is assigned.

L## Mstr Arm Inst

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
3	Master Arm Instant	[COMMAND][1][1]

This authority level permission allows a user to execute the Master Arm Inst function. Refer to *Mstr Arm Inst* on page 61.

Arm Area arms only the area to which the keypad is assigned.

If COMMAND 11 is used, it arms only the area where the keypad is assigned.



Use COMMAND 11 carefully because all Perimeter and Interior points become Instant Armed.

L## Perim Instant

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
4	Perimeter Instant Arm	[COMMAND][2]

Instant arm all Perimeter points, including Delayed points, only in the area where the keypad is assigned.

L## Perim Delay

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
5	Perimeter Delay Arm	[COMMAND][3]

Delay arm all Perimeter Delay point responses only in the area where the keypad is assigned.

L## Watch Mode

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
6	Watch Mode	[COMMAND][6]

Initiate the Watch Mode in the area to which this keypad is assigned.

L## Perim Partial

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
7	Perimeter Partial Arm	[COMMAND][8]

Partially arms only the area where the keypad is assigned.



This function ignores the **A# FA Bypass Max** entry in Area Parameters.



Local Only Reporting: No Closing Report is sent to the central station, but a Perimeter Delay Closing Event is generated in the event log.

L## View Area Stat

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
8	View Area Status	(Menu function only)

View the current arm or disarm status and the not ready to arm status of all areas within the scope of the keypad in this area. The user needs arming and disarming authority.

L## View Memory**Default:** Refer to the program record sheet**Selection:** Blank or E

Function No.	Function Name	Alternate Keystroke
9	View Event Memory	[COMMAND][4][0]

View all memory events that occurred since the last time the system was armed for all areas within the scope of the keypad in this area.

L## View Pt Status**Default:** Refer to the program record sheet**Selection:** Blank or E

Function No.	Function Name	Alternate Keystroke
10	View Point Status	(Menu function only)

View the current status of all points in the area to which this keypad is assigned.

L## Walk Test**Default:** Refer to the program record sheet**Selection:** Blank or E

Function No.	Function Name	Alternate Keystroke
11	Walk Test	[COMMAND][4][4]

Walk Test all Interior or Perimeter Controlled points in the area to which this keypad is assigned.

The following features come with the Walk Test Mode:

- Battery powered control panel only. A Battery Test runs during the whole test to ensure that the battery capacity is capable of supporting the full load of the control panel if AC fails.
 - This test includes 2-sec Bell Test when the Walk Test starts.
 - The test ends when all points are tested or the test times out after 20 min of no activity.
- Local alarm annunciation and event printing; no reports are sent to the central station receiver.
- D1255 Keypad displays a sequential count, and text after each point is activated and restored.
- The keypad displays ALL PTS TESTED and an All Points Tested Event is sent to the central station receiver (if programmed) when the last point is tested.

- If enabled in Routing, Walk Start and Walk End Reports are sent to the central station receiver at the beginning and end of the test.



To Walk Test a Door point connected to a D9210B Access Interface Module, open the door without activating the door sequence or allowing it to time out past the extended shunt time.

L## Fire Test**Default:** Refer to the program record sheet**Selection:** Blank or E

Function No.	Function Name	Alternate Keystroke
12	Fire Test	[COMMAND][5][8]

Fire Walk Test all 24-hour points in the area where this keypad is assigned.

One person can perform a Fire Walk Test without assistance. The following features come with the Fire Test Mode:

- Battery powered control panel only. A Battery Test runs during the whole test to ensure that the battery capacity is capable of supporting the full load of the control panel if AC fails.
 - This test includes a 2-sec Bell Test (Fire Bell relay) for each Fire point that is tested.
 - The test ends when all points are tested or the test times out after 20 min of no activity.
- Local alarm annunciation and event printing; no reports are sent to the central station receiver.
- Automatic smoke detectors reset for all Fire points programmed with **P## Resettable** as **Yes**.
- D1255 Keypad displays a sequential count and the text for the point after each point is activated and restored.
- If enabled in Routing, Walk Start and Walk End Reports are sent to the central station receiver at the beginning and end of the test.



A# Verify Time for Fire points that is programmed with **Yes** for **P## Alarm Verify** is ignored during the Fire Walk Test.

L## Send Report

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
13	Send Report	[COMMAND][4][1] or [COMMAND][4][2]

Send a Test Report from any keypad assigned to an area where the user has authority.

Access Control Functions

Use the following functions to control the doors from the keypad. Users can have authority to access the Door Control and can use all or part of the functions within.



All doors display when this function is selected. This function does not follow the scope of the keypad.

L## Door Control

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
14	Door Control	[COMMAND][4][6]

This item only allows programming access to the following three sub-prompts. It does not affect the user's access to Cycle Door, Unlock Door, and Secure Door.



Cycle Door, Unlock Door, and Secure Door cannot be accessed through the Function List. Door Control must be added to the Function List to access the door control functions, or COMMAND 46 can be used.

The following prompts are sub-functions of Door Control. They become visible in the D5200 Programmer when you Enable Door Control and press [ENTER] on the D5200.



Cycle Door must be enabled for all three sub-functions to operate. If Cycle Door is disabled, all three sub-functions do not operate.

L## Cycle Door

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
(None)	Cycle Door	(Menu function only)

Cycle Door (Menu Function only)

To cycle the doors, press number [1] through [8] on the keypad, corresponding to the door number. For example, pressing [2] and [ENTER] cycles door number 2, which is indicated by C in the display. Refer to "Cycle Door" in *Table 30* on page 71.

Cycle Door allows the user with this authority level to access the CYCLE? 12345678 function.

L## Unlock Door

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
(None)	Unlock Door	(Menu function only)

To unlock or relock a door, press number [1] through [8] on the keypad, corresponding to the door number (refer to "Unlock Door" in *Table 30* on page 71). For example, pressing [2] and [ENTER] unlocks door number 2. The display indicates "U" (for unlock door) with the door number. Select the same door number again and press [Enter] to relock the door.

Unlock Door allows the user with this authority level to access the UNLOCK? 12345678 function.

L## Secure Door

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
(None)	Secure Door	(Menu function only)

Press number [1] through [8] on the keypad, corresponding to the door number to secure or unsecure a door (refer to "Secure Door" in *Table 30* on page 71). For example, pressing [2] and [ENTER] secures door number 2, which is indicated by an X in the display.

Secure Door allows the user with this authority level to access the SECURE? 12345678 function.

Table 30: L## Secure Door-Door Mode Definitions

Door State	Definition
Lock Door	Normal Door: When a door is in the Lock Door state, one can initiate the door sequence using Skeds, CYCLE DOOR?, keypad functions, door requests, and valid token or card requests.
Secure Door	No Access Allowed: When a door is in the Secure Door state, no access is allowed through the door until it is returned to the Lock Door state. The Secure Door state includes Sked and keypad functions.
Unlock Door	Free Access: When a door is in the Unlocked Door state, the door is already shunted and the door strike does not prevent the door from opening. In this state, the user does not need to activate a door request or present a valid token or card.
Cycle Door	Momentary Access: This is a temporary Door Mode in which the door initiates the door sequence as if a valid token or card was read. This state occurs using the keypad and remote programming software (RPS). A sked cannot activate this state.

L## Access Ctl Lvl

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
37	Access Control Levels	(Menu function only)



Changing the Access Control Level in any area affects all users and all doors associated with that level for all areas.

General Functions**L## Chg Display**

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
15	Change Display	[COMMAND][4][9]

Change the display (bright display, dim display, and time display) in the area where this keypad is assigned.

L## Chg Time/Date

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
16	Change Time and Date	[COMMAND][4][5]

Change the date and time for the control panel in this area.

L## Chg Passcode

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
17	Change Passcodes	[COMMAND][5][5]

Change a user passcode.

L## Add User

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
18	Add User	[COMMAND][5][6]

Add or change users, add or change authority levels, add or change tokens or cards.



9210 NOT READY appears if a door controller is not assigned to the keypad used to add or change tokens or cards. Refer to **CC# Assign Door** in Section 2.10.1 Keypad (Command Center) Assignment on page 53.

L## Del User

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
19	Delete User	[COMMAND][5][3]

Delete users.



Although an individual user (001 through 249) can be deleted separately, use caution with this function. User passcodes, tokens or cards cannot be deleted individually within a group. (For example, User 001 has three additional sub-users that use the same authority levels for that group.) When dealing with an individual user, change that user's token or passcode so that other users in the group do not need to be added again.

L## Extend Close

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
20	Extend Close	[COMMAND][5][1]

Change the closing time in the area where the function is entered.

L## View Log

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
21	View Log	(Menu function only)

View all panel-wide events in the control panel's memory log.

L## Print Log

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
22	Print Event Log	(Menu function only)

Print all panel-wide events from the log to the printer in the area where the user is executing this function.



This item can also be accessed using the Service Menu ([9][9][ENT]).

L## User Cmd 7

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
23	User Command 7	[COMMAND][7]

This command can be used in Function Menu. Generate the alarm programmed at COMMAND 7 in the RADXPNTS Handler.

L## User Cmd 9

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
24	User Command 9	[COMMAND][9]

This command can be used in Function Menu. Generate the alarm programmed at COMMAND 9 in the RADXPNTS Handler.

L## Bypass a Pt

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
25	Bypass a Point	[COMMAND][0]

Bypass points with this authority level.

L## Unbypass a Pt

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
26	Unbypass a Point	[COMMAND][0][0]

Unbypass points with this authority level.

L## Reset Sensors

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
27	Reset Sensors	[COMMAND][4][7]

Reset sensors with this authority level.

L## Change Relay

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
28	Change Relays	[COMMAND][5][4]

Manually activate or reset a system relay.



Do **not** use the Chg Relays? function to toggle relays reserved for special functions. Special function relays are Area and Panel Wide Relay functions as well as relays assigned to **CC# Entr Key Rly?**

L## Remote Program

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
29	Remote Programming	[COMMAND][4][3]

Start a remote programming software (RPS) session when the phone rings at the control panel.

L## Move to Area

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
30	Move to Area	[COMMAND][5][0]

Temporarily switch to a different area and perform keypad functions related to that area.

L## Display Rev

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
32	Display Software Revision	[COMMAND][5][9]

Display the control panel model name and software revision. For example:

9412GV3 REV ##.##

L## Service Walk

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
33	Service Walk Test	(Menu function only)

Start a Service Walk Test for all 24-hour Interior or Perimeter Controlled points in the control panel.

Points are not included in this test if:

- Points are in an area that is already in a Walk Test Mode.
- Points are assigned to an area that is not enabled **A# Area On**.
- Points are in an area that is Master or Perimeter armed.

When a Service Walk Test is initiated, one person can test all the points in the control panel without assistance. The following features are provided with the Service Test Mode:

- Display indicates exactly how many points can be tested.
- Battery and bell tests do not occur during this Walk Test.
- The test ends when all points are tested or the test times out after 20 min of inactivity.

- Events print locally without alarm annunciation or reporting to the central station receiver.
- D1255 Keypad displays a sequential count and the text for the point after each point is activated and restored.
- The D1255 Keypad displays ALL PNTS TESTED.
- If enabled in Routing, Service Start and Service End are reported at the central station receiver for the beginning and end of the test.

Point 128 and Point 248 appear as missing. This is normal. These points are used for supervising the Zonex 1 bus (Point 128) and Zonex 2 bus (Point 248). If the Zonex bus has a fault, these points indicate a short.

This function allows viewing of extra points. Extra points occur under two conditions: an extra point is wired electrically to the Zonex bus with a blank **P### Point Index**, or two Zonex devices exist for the same Zonex address.

L## Default Text

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
34	Default Text	[COMMAND][5][7]

Temporarily show the armed state of the area using control panel default text, A# AREA # IS ON, A# NOT READY, A# AREA # IS OFF, and A# ACCOUNT IS ON.

L## Change Skeds

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
35	Change Skeds	[COMMAND][5][2]

Change skeds that can be edited.



Editing of skeds can be restricted by programming **S## Time Edit?** to No.

L## Invisible Walk Test

Default: Refer to the program record sheet
Selection: Blank, or E

Function No.	Function Name	Alternate Keystroke
36	Invisible Walk Test	(Menu function only)

Test all points that are programmed to be invisible and that are within the scope of the keypad without sending reports to the central station. Invisible points must be programmed **P## Invisible Pt** as **Yes**. This walk test mode can test 24-hour points and controlled points.

Invisible Test? allows the user with this L## to start an invisible walk test for all 24-hour interior and posterior controlled points in the area to which this keypad is assigned. When an invisible test is started, one person can test invisible points without assistance.

The following features are provided with the Invisible Test Mode:

- The display indicates exactly how many invisible points are assigned to the area.
- Battery and bell tests do not occur during this walk test.
- The keypad shows point text when invisible points are tested.
- The test ends when all points are tested, or if the test times out after 10 min of no activity.
- Local event printing occurs without alarm annunciation or reports sent to the central station receiver.
- The D1255 Keypad shows a sequential count and text related to the point after each point is activated and restored.
- The keypad shows All PTS TESTED. An All Points Tested Event is sent to the central station receiver (if programmed) when the last point is tested.
- Walk Start and Walk End Reports are sent to the central station receiver for the beginning and end of the test (if programmed in phone routing).

Custom Functions

L## C Function 128 [through 143]

Default: Refer to the program record sheet
Selection: Blank or E

Function No.	Function Name	Alternate Keystroke
128 through 143	Enable Custom Function 128 through 143	(Menu function only)

Execute the desired Custom Function.

Report Levels

L## Force Arm

Default: Refer to the program record sheet
Selection: Blank or E

A user with this authority level can Force Arm.

L## Area O/C

Default: Refer to the program record sheet
Selection: Blank or E

Generates Opening and Closing Reports if the area where this authority level is assigned sends Opening and Closing Reports.

L## Restricted O/C

Default: Refer to the program record sheet
Selection: Blank or E

Generates an Opening Report if a bell is ringing or a Closing Report when force or bypass arming. The area where this authority level is assigned must be programmed for restricted openings and closings (refer to the **A# Restrictd O/C** prompt in Section 2.9.5 *Open/Close Options* on page 43).

L## Perimeter O/C

Default: Refer to the program record sheet
Selection: Blank or E

Generates Perimeter Opening and Closing Reports if the area where this authority level is assigned sends Perimeter Opening and Closing Reports. Refer to the **A# Perimeter O/C** prompt on page 47 in Section 2.9.5 *Open/Close Options*.

L## Send Duress

Default: Refer to the program record sheet
Selection: Blank or E

Generates a Duress Report if the area where this authority level is assigned sends duress. (Refer to the **A# Duress Enable** prompt on page 39 in Section 2.9.5 *Open/Close Options*.)

L## Passcode Arm

Default: Refer to the program record sheet
Selection: Blank or E

Arm an area by entering a passcode and pressing [ENTER].

L## Passcode Disarm

Default: Refer to the program record sheet
Selection: Blank or E

Disarm an area by entering a passcode and pressing [ENTER].

2.11.5 Access Control Levels

L## Security Level

Default: Refer to the program record sheet
Selection: M, P, D, or Blank

M	Users have access rights for this area when the area is in any armed state.
P	Users have access rights for this area when the area is Perimeter Armed or Disarmed but not while the area is Master Armed.
D	Users have access rights for this area only while it is disarmed.
Blank	Users do not have access rights to this area.

Security Level [TOKEN FUNCTION]

When the user presents a token or card at the reader, access is granted only when the user has the authority to enter the area under certain armed conditions.

L## Disarm Level

Default: Refer to the program record sheet Selection: I, D, or Blank	
I	Users change the Master Armed state and Perimeter Armed state to Perimeter Instant. The armed state does not change in other areas, and the armed state does not change if the area is already in the perimeter instant or disarmed state. User needs access level for Master Armed (M) state.
D	Users change the local area's Master Armed state and Perimeter Armed state to the Disarm state. User needs access level for Master Armed (M) or Perimeter Armed (P) state. All areas within the scope of the keypad assigned to the D# CC# Scope in the access handler, and areas to which the user has disarm rights, disarm as programmed.
Blank	Users do not have disarm rights in this area.



Burglar bells are silenced in the local area when a user disarms with a token or card or presents the token or card during an alarm. The user must use a passcode to silence a Fire Bell. Cancel Reports are sent after a valid passcode or token or card silences the bell.



Opening and Closing Reports are sent to the central station receiver if programmed.

For more information on programming this prompt for a shared area, refer to *Access Control Readers Assigned to the Shared Area* in Section 2.9.3 *Shared-Area Characteristics* on page 41.

L## Function Level

Default: Refer to the program record sheet Selection: M, D, C, or Blank	
M	Activate the custom function assigned to the door in this area while the area is Master Armed or Disarmed only.
D	Activate the custom function assigned to the door in this area while the area is Disarmed only.
C	User can activate the custom function assigned to the door in this area while the area is Master Armed, Perimeter Armed or Disarmed.
Blank	User cannot activate the custom function assigned to the door in this area.



When a token or card can also disarm an area, the custom function starts **after** the area disarms.



A user does not require **L## Security Level** or **L## Disarm Level** authority to activate a custom function with a token or card.



Tokens or cards that are used to execute Custom Functions must have a passcode assigned to the corresponding User###.

2.11.6 SIA Duress Passcode Options

GV2MAIN→USER INTERFACE→ Authority Levels
→L## Disarm

GV2MAIN→ USER INTERFACE→ Authority Levels
→L## Send Duress

GV2MAIN→ USER INTERFACE→ Authority Levels
→L## Passcode Disarm

General Programming Information

User Authority Index 14 is programmed by default as a duress disarm profile. When **Duress Option** is configured with a value of **3**, the SIA CP-01 compliant Duress Passcode feature is enabled. With Authority Index 14 assigned to a user passcode in an area, that user has the authority to disarm and send a duress event from that area.

A Duress Disarm user authority index requires:

L## Disarm set to **E**

L## Send Duress set to **E**

L## Passcode Disarm set to **E**

For SIA CP-01 Compliance

Duress Types 1 and 2 (refer to **Duress Type** on page 35) are not allowed for use in SIA CP-01 compliant installations. All duress-capable passcodes must be unique and cannot be derived from other passcodes. To facilitate this uniqueness, user Authority Index 14 is preprogrammed from the factory as an example of duress disarm authority.

2.12 Function List

The Function List is accessed when the user presses [MENU] (or the key corresponding to menu on the D1260) while the keypad shows the idle text. Program as many as 32 **M### Function(s)**.

Each CC # keypad address can display a combination of any of the 32 menu items. The D1255 displays one menu item at a time. The D1260 displays up to two menu items at a time. Each keypad address has one Function List. The function name shown in the Functions column in the program record sheet appears in the keypad display in capital letters. For example, WATCH MODE appears when you select **#6 Watch Mode**.

Menu Item

Default: Refer to the program record sheet
Selection: 1 to 32

Enter the menu item number you are programming. The M## Function displays items sequentially in the order they are programmed. The M1 Function is the first function that appears in the menu and M32 Function is the last function that appears when scrolling through the menu.



Failing to program Menu Item 1 causes COMMAND DISABLED to appear in the keypad display.

M## Function

Default: Refer to the program record sheet
Selection: Blank, 1 to 30, 32 to 35, 37, and 128 to 143

Enter the function number indicated in the “#” column of the program record sheet or next to the function in *Section 2.11 User Interface* on page 60.



Function numbers 128 to 143 are custom functions and show the text programmed for **CF ### Text**.



There is no restriction on how many times you can assign a specific function to the menu. By assigning a specific function more than once, you can assign the same function at different keypads so that their order is different in different areas.

M## CC Address 1 [through 8]

Default:	Refer to the program record sheet
Selection:	Yes or No
Yes	This menu item appears at this keypad address.
No	This menu item does not appear at this keypad address.

Programming this prompt determines at which CC address setting this menu item appears.

2.13 Relay Parameters

Relays provide dry contact (normally open or normally closed) outputs for LED annunciation and other applications as well as wet voltage outputs (12 VDC on or off) for basic alarm system functions (such as Bell Output or Reset Sensors). The applications are endless, but mainly, relays enhance a system's capacity to perform output functions.

- **Panel-Wide Relays:** These relays provide an output related to a panel-wide indication. For annunciation, these relays can indicate system-wide troubles for power and phone. They also provide an overall control panel summary of alarms, troubles, and supervisory conditions.
- **Area Relays:** These relays provide an output by the area to which the relay is assigned. An area can have its own bell and sensor reset indications. Relays can also indicate the area armed state and whether any off-normal conditions, such as a Force Arm, occurred.
- **On Board Relays:** Three on-board 12 VDC voltage outputs provide power when activated on the control panel. These outputs are programmed at the factory as Relays A, B, and C. Typically, Relay A (Terminal 6) is used for the bell, Relay B (Terminal 7) is used for an alternate alarm output (such as another bell), and Relay C (Terminal 8) is used for Sensor Reset (Relays B and C require the optional D136 Relays).
- **Off-Board Relays:** The D9412GV3 can also control 128 (64 for the D7412GV3) dry-contact form C relays when up to sixteen optional D8129 OctoRelay Modules are installed. These relays are used for Area Relay, Panel-Wide Relay, and Individual Point Fault Relays.
- **Relay Follows Point:** Relays can also be used to activate when a point programmed for **P## RlyResp Type** (refer to **P## RlyResp Type** on page 96) is off-normal or in an alarm condition.

- **Relay Reports:** When relay activity is reported to the receiver (refer to *Section 2.3 Routing* on page 16), on-board relays are reported as follows:

A = 253
B = 254
C = 255

The others report as 001 to 128. The Relay Report is RELAY SET RELAY # rrr when the relay is turned on and RELAY RESET RELAY # rrr when the relay is turned off. Relay Reports are also printed on the local printer and stored in the control panel memory log.

- **Controlling Relays:** Relays can activate depending upon conditions that exist with the control panel. In addition, the user can control relays by using the Chg Relay? function, Relay On/Relay Off skeds, and the Remote Account Manager.

Before programming your relays:

- **Do not** use the CHG RELAYS? function to toggle relays reserved for special functions. Special function relays are Area and Panel Wide Relay functions as well as relays assigned to CC Entr Key Rly and **P## RlyResp Type**.
- Relay C is always on. Assigning any other relay (1 to 128, A or B) deactivates Relay C so this output can be used for other functions. When Relay C is programmed for **A# Rest Sensors**, power is always supplied from Terminal 8 of the control panel.
- **Relay Restoration:** The status of relays after programming or resetting the control panel might restore automatically or require manual restoration. All relays are turned off after the control panel resets. The control panel checks certain relay functions every minute and resumes the correct state after the reset. Other relays must be manually set to the correct state using the Change Relay Function (COMMAND 54).

Relay functions that resume the proper state within one minute:

Alarm Bell	Perimeter Fault
Summary Fire	Summary Trouble
Area Armed	Reset Sensors
Fire Bell	AC Fail
Summary Alarm	Phone Fail
Silent Alarm	Summary SupBurg
Area Fault	Battery Trouble
Summary Fire Tbl	Communications Fail
Watch Mode	Summary SupFire

Relay functions that must be reset manually with Change Relay function (COMMAND 54):

Fail To Close	Force Armed
Duress	Log % Full

2.13.1 Area Relays

Each area can be assigned a unique relay number for each of the events listed in this section.

Area**Default:** 1**Selection:** 1 to 8

Enter the area number you are programming.

A# Alarm Bell**Default:** A**Selection:** Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This voltage output relay activates and provides 12 VDC output when a Non-fire point (**P## Fire** is **No**) assigned to this area activates an alarm.



A# Burg Time and **A# Burg Pat** must be programmed in Area or Bell Parameters. This relay activates according to the bell pattern and remains active until the bell time expires or a valid passcode is entered. **P## Silent Bell** must be **No** for the bell to ring upon alarm.

For SIA CP-01 Compliance:

Do **not** set **A# Alarm Bell** to blank. This feature is required for SIA CP-01 compliance.

A# Fire Bell**Default:** A**Selection:** Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This voltage output relay activates and provides 12 VDC output when a Fire point (**P## Fire** is **Yes**) assigned to this area activates an alarm.



Fire Time and Fire Pat must be programmed in Bell Parameters. This relay activates according to the bell pattern and remains active until the bell time expires. **P## Silent Bell** must be **No** in order for the bell to ring upon alarm.



Although Relay C is a valid entry for **A# Fire Bell**, do not program Relay C for this entry. Use Relay A for the **A# Fire Bell**.



To meet UL 864 requirements, set **A# Fire Bell** to a value other than Blank.

A# Reset Sensors**Default:** C**Selection:** Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Unlike the default relay for Alarm Bell and Fire Bell, this voltage-output relay (Relay C) de-activates for 5 sec when the Reset Sensors? function is activated from the keypad or during a Fire Walk Test.



The Reset Sensors time converts from the 5 sec default time to the time programmed in **A# Verify Time** (Section 2.9 Area Parameters on page 4) when a point programmed for **P## Alarm Verify** (Section 4.1 Point Index on page 87) enters an alarm condition.



When sharing one relay to reset sensors in two or more areas, you must program the following. Failure to do so causes TROUBLE PT ### for all point types programmed as **P## Resettable**.

- **CC # Scope** must include all areas that share the relay.
- **L## Reset Sensors** authority must be assigned to the passcode that activates the COMMAND 47 or Reset Sensor function.
- **A# Verify Time** must be the same number of seconds for all areas that share the relay.



To meet UL 864 requirements, set **A# Reset Sensors** to a value other than Blank.

A# Fail to Close

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This relay activates when the Closing Window expires for the specified area. It remains active until midnight, another Closing Window starts, or the control panel resets, whichever occurs first. When **Perimeter Relay** (refer to page 142) is set to **Yes**, the **A# Fail to Close** prompt becomes **A# Perimeter Relay**.

A# Force Armed

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This relay activates when this area is Force Armed. It remains active until the area disarms or the control panel resets.



If Force Bypassing is required during Perimeter Arming, this relay does not activate.

A# Watch Mode

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This relay activates when a Controlled point programmed for **P## Watch Point** is faulted in the specified area while the area is in Watch Mode and the point is not armed. It remains active for 2 sec after each point is faulted.

A# Area Armed

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This relay activates when the specified area becomes Master Armed. The exit delay must expire before the relay activates. The relay remains active until the area disarms. It does not deactivate during the entry delay time.

If multiple areas use the same relay, the relay activates when all areas are armed. It deactivates when the first area disarms.

The **A# Area Armed** relay function can provide visual feedback at a key switch station. Attach a LED to the output of a D8129 Module programmed for this function.

A# Area Fault

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates whenever a controlled (**P## Type 1, 2, 3** only) Perimeter or Interior point is faulted. The relay remains active until all Perimeter and Interior points in the area are normal.



Keyswitch area armed status with LEDs: Use a D8129 Module and connect an LED to indicate that the area is not ready to arm.

A# Duress Relay

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when a Duress alarm is generated from a keypad assigned to the specified area.



Burg Time needs a bell period programmed and **A# Duress Enable** must be **Yes**. This relay activates when the Burg Bell starts and deactivates when the Burg Bell time ends. The Burg Bell pattern has no effect on this relay function.

A# Perim Fault

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when a Controlled Perimeter point (**P## Type 1**) assigned to the specified area is faulted, regardless of the armed state of the area. This relay provides a steady output until all Perimeter points in the area return to normal.



This relay does not activate on interior faults. To detect all area point faults, program all points as Perimeter points in the area where this relay is assigned.

A# Silent Alarm

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

This relay activates when a point assigned to the specified area and programmed for **P## Silent Bell** goes into alarm.

2.13.2 Panel-Wide Relays

The following eleven relay options activate when they occur anywhere in the control panel. They are not restricted by area boundaries.

AC Failure

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when the control panel responds to an AC power failure as programmed in **AC Fail Time** in *Section 2.5 Power Supervision* on page 28. This relay automatically resets when AC power restores.



Use this relay to create audible annunciation. Enable the keypad's trouble sounders for all applications except commercial fire systems.

Battery Trouble

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when battery voltage falls below 85% of capacity (12.1 VDC) for a fully charged (13.8 VDC) battery, or when the battery is in a missing condition. This relay automatically resets when battery power restores.



Use this relay to create audible annunciation. Enable the keypad's trouble sounders for all applications except commercial fire systems.

Phone Fail

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when a telephone line failure occurs. A time must be entered in Ph Supv Time (refer to *Section 2.2 Phone Parameters* on page 12) for this relay to activate. This relay resets automatically when restoration of the phone line(s) occurs.

Comm Trouble

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when a control panel cannot communicate a report after making ten attempts to each routing destination. At the same time, COMM TROUBLE RT ## displays at the keypad. This relay automatically resets when a report is sent successfully.



Use this relay to report primary digital report failure to an alternate communication device.

Log % Full

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Enter the number of the relay that activates when the log reaches the programmed percentage of its capacity as programmed in the **Log % Full** prompt under GV2MAIN. This relay provides a steady output until a Get Log and Set Pointer is executed from the remote programming software (RPS).

Summary Fire

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Enter the number of the relay that activates when any Fire point in the system (**P## Type 0, P## Fire Yes**) enters into alarm. This relay provides a steady output until all Fire points in the system return to normal. Refer to **Fire Summary Sustain** on page 139 for details on alternate operation.

Summary Alarm

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Enter the number of the relay that activates when a Non-fire point enters into alarm. This relay provides a steady output until the alarm is acknowledged by a valid passcode, then cleared from alarm memory with an acknowledgment at the keypad.



This relay does not activate for silent and invisible alarms.

Summary Fire Tbl

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when any Fire point in the control panel is in trouble, or if a Fire Supervision point is missing. This relay provides a steady output until all Fire points restore to a normal condition.

Summary SupFire

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when any Fire Supervisory point in the control panel is in a supervisory condition (off-normal). This relay provides a steady output until all Fire Supervisory points are restored to a normal condition.

Summary Trouble

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when any Non-fire point in the control panel is in a trouble condition. This relay provides a steady output until the user at the keypad acknowledges the trouble.

Summary SupBurg

Default: Blank
Selection: Blank, 1 to 128 (1 to 64 for D7412GV3), A, B, or C

Activates when any Non-fire Supervisory point in the control panel is in a supervisory condition, or if a Supervisory Burg point is missing. This relay provides a steady output until the user at the keypad acknowledges the condition.

3.0 RADXUSR1/RADXUSR2

3.1 Passcode or Token Worksheet

These programming items assign:

- a passcode to user groups 001 to 249,
- areas by authority level, and
- a User Group Window.

Two handlers in the D5200 Programmer are used to program the users:

- RADXUSR1 Handler programs users 000 to 124.
- RADXUSR2 programs users 125 to 249 (D9412GV3 only).

3.1.1 User Groups

For the D9412GV3, there are 249 groups (99 groups for the D7412GV3) consisting of one user with a passcode and token (master) and three users with tokens or cards but not a passcode (sub-user). All users in the group share the same authority level as the master user.

3.1.2 Passcodes

In a control panel with factory default settings, only the master user has an assigned passcode. A passcode can be three to six digits. Entering three digits in **User ###** chooses the user. Programming the **U001 Passcode** assigns a passcode to the master user. Sub-users cannot use the passcode. Do not assign tokens or cards to User ID 0 (zero), which is reserved for the service passcode.

Passcode Tamper

If a user enters six consecutive invalid passcodes at the same keypad, the control panel sends a User Code Tamper report to the central station. The invalid passcode count resets when a valid passcode is entered at the same keypad. Refer to R# Usr Code Tamper in *Table 12* on page 18 for information on enabling this report.

The passcode tamper condition is also reported in a manually initiated Extended Test Report and to RPS through control panel diagnostics. As a result, the tamper condition is reset after the successful completion of a manual report or when disconnecting from an RPS session. The tamper condition is not reset when the control panel reboots.

3.1.3 User Group Window

Use **U### User Group** to enable and disable the **U### Passcode** for up to eight different time periods throughout the day. Assign the number (1 to 8) programmed in **U### User Group** to a **User Windows #**. If the user is outside a window, COMMAND DISABLED appears on the keypad after the user enters the passcode and presses [ENTER].



This window does not affect tokens and cards. It only affects the passcode of the master user.



When using the Add/Change User function at the keypad, the authority levels

and the changes made affect the master user's passcode and the entire group's token or cards.

When using the ACCESS CTL LVL function at the keypad, the whole group is affected by whether or not the level is on or off for access control functions only.

When using the DELETE USER? function, the whole group is deleted. You cannot delete each user within the group individually. Use the ADD/CHG USER? function to change a user token or card instead of deleting the whole group.

3.1.4 User Name

Each user group can be assigned one **U### Name**. This name is logged and sent to the central station for all the users in the group. The user ID is used to differentiate which user's token or card was executed.



When using a D1260 Keypad, User 249 text is used for contact information text (such as telephone numbers). If a D1260 is installed on the system, do not use User 249 for user ID information.

3.1.5 Tokens and Cards

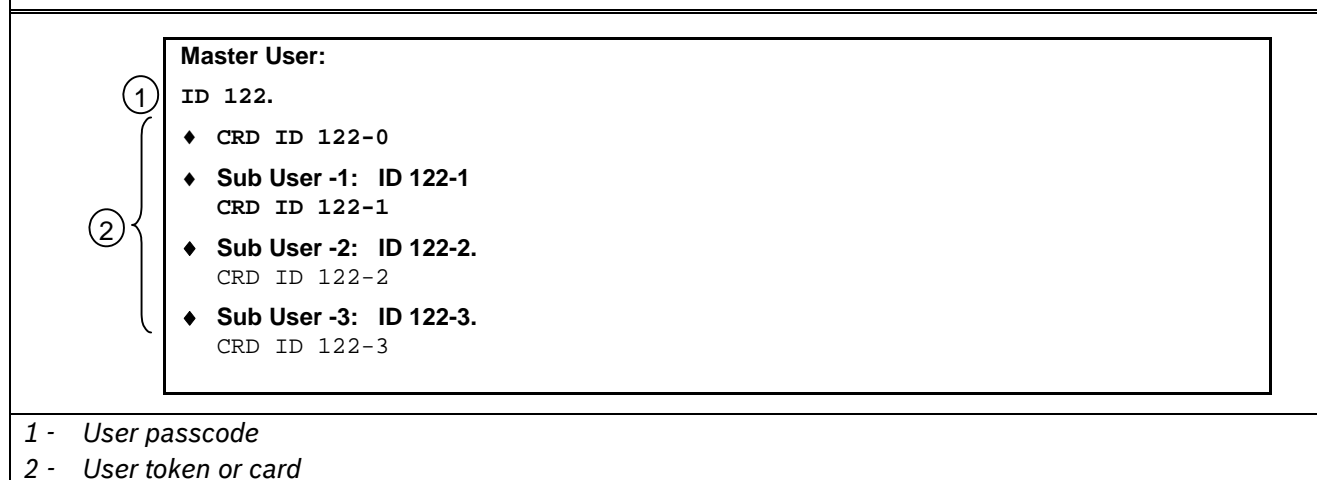
The master user assigned the passcode can also be assigned a token or card by programming the **U### Mstr Site** and **U### Mstr Crd Data**.

Three more tokens or cards are assigned to the user group for sub-users using the **U### SU# Site** and **U### SU# C/D**.

3.1.6 Reporting and Logging

Modem Format must be **Yes** for the following reports sent to the central station. Regardless of the reporting format, they log and print at the local printer as shown in *Figure 4*. Each sub-user is identified by the master user's three-digit number plus an extension of 0, 1, 2, or 3. These numbers are called Sub-user ID Codes. shows all the users for User Group 122 as they would appear.

Figure 4: User Group 122 Example



In reporting systems using modem format, all three digits of the User ID Code are transmitted to the central station with appropriate reports. Central station automation computer systems can accept only Zonex and Comex style User IDs. Refer to **Point/User Flag** in *Section 2.1 Phone* on page 11.

User

Default: 001

Selection: 000 or 001 to 249 (001 to 099 for the D7412GV3)

Enter the User number you are programming.



User 000 is the Service Authority Level (Level 15). You cannot change the programming for user 000.

Only the Service Authority Level (User 000) can delete User 000. When a user other than User 000 tries to delete the passcode for User 000, the keypad displays NOT IN USE.

User 000 cannot be added or changed at the keypad whether it exists or not.

U### Passcode**Default:** Refer to the program record sheet**Selection:** Three to six digits (0 to 9)

Enter three to six digits to enable a passcode for the master user in this group.



To meet UL 864 requirements, enter at least one Passcode.



User I.D.000 is the reserved user for service personnel. The default service passcode is 123.

The programmer does not allow you to enter any passcode number that might conflict with a duress passcode. The programmer reserves the passcode number plus 1, duress passcode number plus 2, passcode-number minus 1, and passcode number minus 2.

For example, when a passcode of 654321 is entered, 654322, 654323, 654320, and 654329 are reserved and are not available to other users.



The authority to silence a bell is granted to all passcodes regardless of their authority level assignments. A user passcode can silence a Fire or Burg bell as long as any authority level is assigned to the area where the bell can be silenced.

U### User Group**Default:** Blank**Selection:** Blank, 1 to 8

Create a group of up to 249 users (99 for the D7412GV3) whose combinations can be enabled and disabled using an automatic user window. This is the number entered into the **W# User Group** for any active **W# User Window**. Multiple windows can be programmed for one user group (up to eight) within one 24-hour period. For example, if User Group 1 has a window running from 8:00 AM (start time) to 4:00 PM (stop time), the users for that group can use their passcodes only between that time. Between 4:00 PM that day and 8:00 AM the next day, the users cannot use their passcodes.



To enable this user's passcode at all times, leave **U### User Group** blank.

User Group Window times cannot be changed from the keypad. When a window is assigned to a user group, the users in that group rely on the window to be active (within the start and stop times) for their passcodes to function. The only way to disable the window is by reprogramming the control panel from the D5200 or remote programming software (RPS).

U### Area 1 [through Area 8] Auth**Default:** Refer to the program record sheet**Selection:** 1 to 14 or Blank

Assign an authority level to the user for this area. Blank means the user has no authority in this area.



To meet UL 864 requirements, assign a valid authority level to the Passcode to silence bells.

U### Name**Default:** Refer to the program record sheet**Selection:** Sixteen alphanumeric characters

Enter Alphabetic-characters A to Z in capital letters
Period (.), comma (,), percent (%), parentheses [],
equal (=), greater or less than (< >), exclamation (!),
braces {}, apostrophe ('), carat (^), grave accent (`),
tilde (~), semi-colon (;), and colon (:) are not allowed.

Enter up to sixteen characters of text for this user group.



Programming this group with a departmental, team, or function name identifies all the users in this group in a function related manner, such as ENGINEERING.

Card Data Format

The D9412GV3/D7412GV3 and D9210B Controller comply with the 26-bit Wiegand card data format. In essence, the format consists of 26 bits (3.2 bytes) of data. The first bit is used for the even parity. The next 8 bits (first byte) is used for the **U### Site Code**. The next 16 bits (second and third byte) are used for the **U### Card Data**. The last bit is used for the odd parity.

As long as the reader and the tokens or cards you use are compatible with 26-bit Wiegand format, they function with this system.

Use only the readers identified as being compatible with the D9210B door control module. Refer to the *D9210B Operation and Installation Guide* (P/N: 32206) for information on these readers.

For more information, refer to the *Security Industry Association (SIA) Access Control 26-bit Wiegand Reader Interface Standard*.

U### Mstr Site**Default:** Blank**Selection:** 000 = (0) to 254 or Blank (255)

Master User ### Site Data: Enter the first three decimal numbers on the back of the token or card. This is the first byte (bits 2 through 9) of data for a 26-bit Wiegand card. This is called the site number. Tokens and cards with a site code of 255 are not compatible with the D9412GV3/D7412GV3 Control Panels.



Converting hexadecimal to decimal: If your card label contains letters as well as numbers, the number is hexadecimal.* Convert the hexadecimal number to decimal using your calculator. If you cannot convert in this way, use the reader and the Add/Chg User? Function to add the tokens or cards.

Perform the following test to confirm that you can convert properly:

Use 319EB0 as the hexadecimal number. On your calculator, press [HEX]. Enter all the hexadecimal characters into the calculator. Press [DEC] and your hexadecimal characters convert to the following eight digits: 03251888. The site number is 032. Enter it in **U### Mstr Site**. Your card data is 51888. Enter it into **U### Mstr Crd Data**.

* A hexadecimal number can contain all numerals. If the code does not work, try converting the number from hexadecimal to decimal.



Always tag your tokens before adding them to the system so you do not mix them up. Use the CRD ID ###-# number to index them.

U### Mstr Crd Data**Default:** Blank**Selection:** 00000 = (0) to 65534 or Blank (65535)

Master User ### Card Data: Enter the remaining five decimal numbers on the back of the token or card. This is the second and third byte (bits 10 through 25) of data for a 26-bit Wiegand card. This is called the card data.

You must program **U### Mstr Site** before programming this prompt.

U### SU1 through SU3 Site**Default:** Blank**Selection:** 000 = (0) to 254 or Blank (255)

Sub-users one through three site data.

U### SU1 through SU3 C/D**Default:** Blank**Selection:** 00000 = (0) to 65534 or Blank (65535)

Card data for sub-users one through three.

4.0 RADXPNTS

4.1 Point Index

Use this programming module to construct personality types for points used in the system. The Index numbers are used in Point Assignments. Each unique point index number determines the control panel's responses to specific conditions occurring on the Protective points.

The NEW RECORD program contains default entries and descriptions that match RPS defaults for point indexes. Refer to the *D9412GV3/D7412GV3 Program Record Sheet* (P/N: F01U143072) for defaults.


Point Index

Default: 1
Selection: 1 to 31

The number of the point personality you are programming. You can define up to 31 individual personalities.

P## Type

Default:	Refer to the program record sheet
Selection:	0 to 9, or 11
P ## Type	Description
0	<p>24-hour: A 24-hour point is not turned on and off from a keypad. 24-hour points are armed all the time, and can be used for fire protection (refer to the P ## Fire Point prompt in <i>Section 4.2 Point Responses</i> on page 91), panic, medical, and police alerts.</p> <p>24-hour protection for fire doors, roof hatches, and so on. Instead of programming this type of protection as a 24-hour point, consider using a Perimeter point type with a Point Response of 9 to E. 24-hour points do not show faults when an arming function is entered, but Perimeter points do. When programming this type of protection, consider also using the Buzz on Fault and Local While Disarmed options.</p>
1	<p>Perimeter: Perimeter points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using Perimeter-Arming functions) separately from points programmed as interior. This lets the user partially arm the system to establish Perimeter protection while occupying the interior of the protected premises.</p> <p>Perimeter points can be programmed to activate entry delay time. If the point activates entry delay, it can also activate an entry tone.</p> <p>When a Perimeter point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Perimeter point is faulted, the control panel compares the remaining entry delay time to the time programmed for the second Perimeter point. If the second Perimeter point's entry delay time is less than the remaining time, it shortens the entry delay time.</p> <p>Perimeter points programmed for an instant point response, generate an alarm immediately when faulted, even during entry or exit delay.</p>

P ## Type	Description
2	<p>Interior: Interior points are armed only by master arming the area. They are not armed when using Perimeter Arming functions. These points are typically used to monitor interior detection devices such as interior doors, motion detectors, photoelectric beams, and carpet mats.</p> <p>Instant Interior Points: Interior points are usually programmed for an instant alarm (refer to <i>Section 4.2 Point Responses</i> on page 91). Points programmed for instant alarms generate alarms immediately, even during entry or exit delay.</p> <p>Delayed Interior Points: Interior points can be programmed for a delayed point response. A delayed response means that if the point is faulted while the area is armed, it activates entry delay. It does not generate an alarm until entry delay expires.</p> <p>When an Interior point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a fault occurs for the Interior point, the control panel compares the remaining entry delay time to the time programmed for the Interior point. If the Interior point's entry delay time is less than the remaining time, it shortens the entry delay time.</p> <p>Delayed points can also activate an entry tone at the keypad (refer to the P## Ent Tone Off prompt in <i>Section 4.2 Point Responses</i> on page 91).</p> <p>In some cases, you might need to create an Interior point that causes an instant alarm if the entry delay is not started first. Use Interior Follower to create this type of protection.</p>
3	<p>Interior Follower: Interior Follower points are armed only by master arming the area. They are not armed when using Perimeter-Arming functions.</p> <p>An Interior Follower point does not create an alarm if it has a fault while the area is in entry delay. An Interior Follower does not change the amount of remaining entry delay time.</p> <p>If no entry delay is in effect when a fault occurs for the Interior Follower, it creates an instant alarm.</p> <p>You must program a delayed Point Response (4, 5, 6, 7, or 8) for an Interior Follower point. The control panel ignores the entry in P## Entry Delay for an Interior Follower point.</p> <div>  <p>Increasing the debounce count for Interior Follower points might be necessary to prevent Interior Follower points from entering into alarm before the control panel recognizes that a Perimeter Delay point was faulted. Program the Interior Follower's debounce for one number higher than the debounce count on Perimeter delay.</p> </div>

P ## Type	Description
4*	<p>Keyswitch Maintained: Program P## Pt Response as 1. Do not connect initiating devices to a Keyswitch point.</p> <p>Normal: The area is disarmed.</p> <p>Short: When this point changes from normal to open, the area arms.</p> <p>Open: A short is a trouble when the area is disarmed. A short is an alarm when the area is armed. When this point changes from shorted to normal or open, it restores.</p> <p>Program Point Response as 2, the point responds as follows:</p> <p>Normal: When this point changes from open to normal, the area arms.</p> <p>Open: The area is disarmed.</p> <p>Short: A short is a trouble when the area is disarmed. A short is an alarm when the area is armed. When this point changes from shorted to normal or open, it restores.</p> <p>Trouble and Restoral Reports are not sent if Local While Disarmed is Yes. Alarm and Restoral Reports are not sent if Local While Armed is Yes.</p>
5*	<p>Keyswitch Momentary: Used for area arming and disarming. Point Response must be programmed 1. Do not connect initiating devices to a Keyswitch point.</p> <p>N→S→N: When this point momentarily changes from normal to shorted to normal, it toggles the armed state of the area.</p> <p>Open: An open is a trouble while the point is disarmed. An open is an alarm while the point is armed. When this point changes from open to normal, it restores.</p> <p>Trouble and Restoral Reports are not sent if Local Disarmed is Yes.</p>
6*	<p>Open/Close Point: Used for point arming and disarming. Point Response must be programmed 1. Local bells are silenced through the keypad.</p> <p>Normal: The point is armed and sends a Point Closing Report. A Point Closing Report is not sent if Local Armed is Yes.</p> <p>Open: An open is an alarm when the point is armed. An open is a trouble when the point is disarmed. Alarm and Restoral Reports are not sent if Local Disarmed is Yes.</p> <p>Short: The point is disarmed and sends a Point Opening Report. A Point Opening Report is not sent if Local Armed is Yes.</p>

* **Keyswitch Points: Special rules apply to points used for Keyswitch functions.** These special point types do not respond the same way to the point response entry as Point Types 1, 2, and 3. Responses for Keyswitch point types are described in *Section 4.2 Point Responses* on page 91.

P ## Type Selection	Description
7*	<p>D279 (O/C Non-Priority): The D279 provides point arming and disarming independent of the area arm state. A non-priority D279 point arm state does not affect the area arm state. Point Response must be programmed 1. Local bells are silenced through the keypad. For bell control at the D279, use <i>P## Type 8</i>.</p> <p>Open the W1 jumper on the D279 to send Point Opening and Point Closing Reports. If the D279's W1 jumper is closed, no Open or Close Report is sent, regardless of control panel programming.</p> <p>Normal: The point is armed and sends a Point Closing Report. Point Closing Report is not sent if Local Armed is Yes.</p> <p>Open: The point is disarmed and sends a Point Opening Report. A Point Opening Report is not sent if Local Armed is Yes.</p> <p>Short: A short is an alarm when the point is armed. A short is a trouble when the point is disarmed. Alarm and Restoral Reports are not sent if Local Disarmed is Yes.</p>
8*	<p>D279 (O/C Priority): The D279 provides point arming and disarming independent of the area's arming state. A priority D279 point must be armed before an area can be armed. Program Point Response as 2.</p> <p>Open the W1 jumper on the D279 to send area Opening and Closing Reports as programmed in Area Parameters and to provide bell control. If the D279's W1 jumper is closed, no Area Open or Area Close Report is sent, and alarm bells can only be silenced from a keypad, no matter how the control panel is programmed.</p> <p>Normal: When this point changes from open to normal, the area arms.</p> <p>Open: The area is disarmed. The alarm bell silences if an alarm occurred while the area was armed.</p> <p>Short: A short is a trouble while the area is disarmed. A short is an alarm while the area is armed. When this point changes from shorted to normal or open, it restores.</p>
9*	<p>Easikey: This point is programmed for access. Program Point Response as 1. If the system is Master Armed or Perimeter Armed (with or without delays), presenting a valid token to the Easikey reader shorts the point and disarms its assigned area. Presenting a valid token in a disarmed state does not clear trouble or alarm memory or rearm the area.</p>
11	<p>Aux AC Supervision: This point type monitors the AC power of an auxiliary power supply. When the point is in an off-normal state, the control panel waits for the time programmed in AC Fail Time before generating a Point Trouble. If P## Fire Point is set to Yes, the off-normal condition results in a Fire Trouble. This point type does not use P## Point Response; therefore, no alarm condition occurs. If this point type is bypassed, 24 HOUR PT BYPASSED is shown on the keypads.</p>

* **Keyswitch Points. Special rules apply to points used for Keyswitch functions.** These special point types do not respond the same way to the point response entry as Point Types 1, 2, and 3. Responses for keyswitch point types are described in *Section 4.2 Point Responses* on page 91.

4.2 Point Responses

4.2.1 Applications for Point Responses 9, D, and E:

Combine Point Responses 9, D, and E with Perimeter point types to create more flexible 24-hour protection. Unlike 24-hour points, a faulted Perimeter point with a Point Response of D and E displays at the keypad when arming. Like a 24-hour point, a point programmed this way can generate alarms whether the area is armed or disarmed.

Combining Point Response 9 with the Local While Disarmed feature provides off-site reporting when the area is armed, but only local alarm annunciation when the area is disarmed.

Combining Point Response 9 with the Local While Armed feature provides off-site reporting when the area is disarmed, but only local alarm annunciation when the area is armed.

Point Response E: Use this setting for Zonex or ASIC motion detectors. The control panel can report troubles while Master Armed.

Point Response F: Does not sound at local keypads but activates **P## RlyResp Type 1** and keypad faults. To annunciate the off-normal state at a keypad, program **Disp as Dvc** as **Yes** and optionally set **BuzzOn Fault** as 1 or 2. This point response does not generate alarms or activate an alarm relay.

Point Response 8, 9, A, B, and C: These point responses provide supervisory (24-hour) reporting.

4.2.2 Characteristics of a Fire Point:

Reporting: When a group of events occurs, the control panel routes and prints out Fire Reports first.

Visual Annunciation: FIRE TROUBLES continues to scroll until the trouble clears. When acknowledged, a FIRE TROUBLE scroll notifies the end user that a Fire point, or group of Fire points, is still in trouble. Panel-Wide Relays, **Summary Fire**, and **Summary Fire Tbl** activate if a relay is assigned when any Fire point enters into alarm or is in trouble.

Audible Annunciation: A Fire point activates the **A# Fire Bell** relay programmed in Relay Parameters. The amount of time and the pattern of the relay activation is programmed by area in **Bell Parameters**, **A# Fire Time**, and **A# Fire Pat**.

Supervisory: A Fire point can send a Fire Supervisory Report and activate the **Summary Fire Sup** and **Summary Fire Tbl**, Panel-Wide Relays with a **P## Response** of 8-9-A-B-C.

Alarm Verification: A Fire point can delay an alarm by the length of time programmed in **A# Verify Time** in the Area Parameters. Combined with **A# Resettable**, a Fire point also resets the electrical circuit for the amount of time programmed.

Reset Sensor: A fire device that requires resetting can be manually reset using the reset sensor relay for the area to which it is assigned.

Fire Walk: Use the Fire Walk function to test Fire points in the system. The Fire Walk Test automatically resets each point for 5 sec when the point is activated, and rings the Fire Bell for 2 sec.



To provide an audible tone for a restored Fire Supervisory point, use **P## RlyResp Type 1** and connect the corresponding relay to a visual annunciator.

P## Pt Response**Default:** Refer to the program record sheet**Selection:** 0 to F**Controlled (Non-24-Hour Points)**

Point Response		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Armed	Open	I	I	I	I	D	D	I	I	D	I	I	I	I	I	T	
Armed	Short	I	I	I	I	I	I	D	D	D	I	I	I	I	I	I	
Disarmed	Open		T		T				T		I	I	T	I		T	
Disarmed	Short			T	T		T				I	T	I		I		

24-Hour Points

Point Response		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Open		I	T	I	T			I	T	S	T	S		S			
Short		I	I	T	T	I	T			T	S		S	S			

Key:

- I = Instant alarm
- D = Delayed alarm
- T = Trouble
- S = Supervisory
- Blank = Audible or visual response

If this time expires before disarming, or if the point is configured with an instant response (I), an alarm occurs.



Make entries in 5 sec increments. The programmer does not allow off-increment entries.

Example of Controlled point:

Point Type = 1

Point Response = 8

Perimeter point with delayed alarm response when armed (opened or shorted) and no response when disarmed.

Example of 24-hour point:

Point Type = 0

Point Response = 8

When the control panel is in Entry Delay, entering a valid Passcode disarms the system as soon as the last digit of the Passcode is entered. No other keys are required. When the control panel is in Exit Delay or is armed, entering a valid Passcode must be followed by the [ENTER] or [ENT] key.



If another Perimeter or Interior Follower Delay point trips while the area is already in entry delay, the control panel adjusts the delay time to the Delay point with the least amount of delay time.

When a user enters an area, a Perimeter point is faulted and the entry delay starts. If an interior point must fault during entry delay to allow the user to disarm the area at a keypad, program **P## Type** as 3 (Interior Follower).

P## Entry Delay**Default:** Refer to the program record sheet**Selection:** 5 sec to 600 sec

Use this option to enter the amount of entry delay time that a user has after faulting a Controlled point (**P## Type 1, 2, 3**) with a delayed response (D) (**P## Pt Response**) of 4, 5, 6, 7, or 8. DISARM NOW appears for the duration of the time programmed when the point is faulted in the delay condition.



The D1255 alternates between DISARM NOW and the point text of the point that caused the area to enter into entry delay.

For SIA CP-01 Compliance:

P## Entry Delay must be between 30 sec and 240 sec.

P## Ent Tone Off

Default:	No
Selection:	Yes or No
Yes	Disables the entry delay tone when this perimeter point is faulted. This is intended for use with points set to P## Type 1 (Perimeter).
No	A tone sounds at keypads when this point starts entry delay.

This option enables and disables the entry delay warning tone for this point.



Do not set points to **No** if they are actually used to notify the user to disarm the system. The possibility of false alarms increases if the entry delay warning is not used.



Entry Tone can also be turned off when programming your CC Entry Tone, in *Section 2.10 Keypad (Command Center)* on page 50, that allows you to manage the tone by keypad.



You might want to disable the entry tone in high security applications where you do not want to annunciate entry delay.

P## Silent Bell

Default:	No
Selection:	Yes or No
Yes	Activate the Silent Alarm Relay when this point enters into alarm. Keypads do not sound the alarm tone for Non-fire points.
No	Activate either the Fire Bell relay or Alarm Bell relay and sound the alarm tone at keypads when this point enters into alarm. If this is a Fire point, it activates the Fire Bell relay programmed in Relay Parameters. Otherwise, it activates the Alarm Bell relay. The amount of time and pattern of the relay activation is programmed by area in Bell Parameters.



To meet UL 864 requirements, set this parameter to **No**.



If you want this point to ring the bell because the message failed to reach the central station receiver, program **P## Audible After 2 Failures** as **Yes**.

P## Ring Til Rst

Default:	No
Selection:	Yes or No
Yes	The relay programmed to provide fire alarm output for this point cannot be de-activated until the point restores to normal.
No	The relay programmed to provide fire alarm output for this point can be de-activated before the point restores to normal.

Use this option to determine if the bell continues to ring until the Fire Bell time expires. The point returns to a normal condition when the user acknowledges the alarm to silence the bell.



If the point restores and the fire alarm is not silenced from the keypad, the fire alarm output continues until Fire Bell time expires. If the point does not restore, the fire alarm output continues even after bell time expires.



Use this option for fire applications to meet the requirement that audible alarms cannot be silenced until the fault condition clears or the Fire Bell time expires.

P## Audible After 2 Failures

Default:	No
Selection:	Yes or No
Yes	A# Burg Alarm relay activates after two failed attempts.
No	P## Silent points do not cause the A# Burg Alarm relay to activate even if the report does not get to the central station receiver.

When set to Yes, if the report fails to reach the central station after two attempts, a silent alarm rings the **A## Burg Alarm** bell. A silent alarm is generated when a point with **P## Silent** set to **Yes** is faulted while armed.



When a point programmed for **P## Silent Bell** is faulted, the timer for the **A# Burg Time** starts, even though the bell is not yet ringing. As much as 3 min can elapse before the second attempt fails. Ensure that **A# Burg Time** is programmed to provide the amount of bell time you need, minus the additional 3 min that might elapse before the bell actually begins to ring.

program **P## Silent Bell** as **Yes**.



If a user enters a valid passcode while a bell is ringing for an invisible alarm, the keypad shows ALARM SILENCED.

P## Invisible Pt

Default:	Refer to the program record sheet
Selection:	Yes or No
Yes	Keypads do not display alarm activity from this point.
No	Activity from this point is visible at the keypads.



To meet UL 864 requirements, set this parameter to **No**.

Use this option to determine whether the point appears in the keypad display upon an alarm condition. For LED keypads, the LED does not illuminate upon an alarm condition. Point text appears and annunciation is made for Invisible points programmed for a trouble condition in point response.



To prevent the keypad alarm tone and the **A# Burg Alarm** bell from sounding,

P## Buzz On Fault

Default: Blank		
Selection: Blank, 1 to 3		
Selection	Operation for Controlled Points (Point Types 1, 2, and 3)	Operation for 24-hour, Fire and Aux AC Supervision Points (Point Types 0 and 11)
Blank	The point buzzes at the keypad only if it enters into the trouble condition indicated in the P## Point Response .	Same as operation for controlled points
1	The point generates a Buzz Until Restore at the keypad for any fault condition while the point is disarmed . The buzz continues until the point restores and the user acknowledges the condition using a passcode or COMMAND 4. The point must be normal before the user can silence the buzz.	The point generates a Buzz Until Restore at the keypad for any fault condition regardless of the armed state . The buzz continues until the point restores and the user acknowledges the condition using a passcode or COMMAND 4. The point must be normal before the user can silence the buzz.
2	The point buzzes at the keypad for any fault condition when the point is disarmed . The user can silence the buzz before the point returns to normal.	The point buzzes at the keypad for any fault condition regardless of the armed state . The point does not need to be normal before the user can silence the buzz.
3	The point buzzes at the keypad for any fault condition when the area is disarmed. The user cannot silence this buzz, but it silences automatically when the point is restored. If the fault condition results in a trouble response, the keypad continues to buzz even after the user acknowledges the condition if the fault is still present.	The point buzzes at the keypad for any fault condition regardless of the armed state . The user cannot silence this buzz, but it silences automatically when the point is restored. If the fault condition results in a trouble response, the keypad continues to buzz even after the user acknowledges the condition if the fault is still present.



Points bypassed (by the user, Sked, Swinger Bypass, or RPS) do **not** generate a Buzz On Fault condition at the keypad.



The buzz does not automatically stop when the point is restored when using Option 1 or 2. The user must acknowledge the buzz before the buzz stops. However, when using Option 3, the buzz stops automatically when the point restores to normal without user intervention.



If a point with the type of 11 Aux AC Supervision is bypassed, 24 HOUR PT BYPASSED is shown on the keypads.

P## Watch Point

Default:	Refer to the program record sheet
Selection:	Yes or No
Yes	Activates Watch Mode responses if the point is faulted while the control panel is in Watch Mode.
No	Does not activate Watch Mode responses for this point.

Use this option to allow a Controlled point to generate a watch tone while the area is disarmed and not faulted to a trouble or alarm condition.

P## RlyResp Type

Default:	Refer to the program record sheet
Selection:	Blank, 1 to 2
Blank	Point state does not affect the operation of the corresponding relay.
1	Relay Follows Point: The relay corresponding with this point activates when the point is faulted to any off-normal condition, even if the point is bypassed. The relay automatically resets when the point returns to normal.
2	Relay Latches: The relay corresponding with this point latches when the point enters into an alarm condition. This relay provides a steady output until the alarm is acknowledged by a valid passcode, then cleared from alarm memory with an acknowledgment from the keypad.

Use this option to cause a relay (1 to 127 for D9412GV3; 1 to 64 for D7412GV3) to respond when a corresponding point with the same number (1 to 127) is faulted. This requires connecting D8129 OctoRelays to Zonex Bus 1 and Zonex Bus 2 (D9412GV3 only). Refer to the address settings on the back of the *D9412GV3/D7412GV3 Program Record Sheet* (P/N: F01U143072).



Point 128 is reserved for use other than an actual point. Only the first 127 points can have an associated relay. Relays are not available for Points 129 to 247.



Do **not** use the Chg Relays? function to toggle relays reserved for special

functions. Special function relays are Area and Panel Wide Relay functions as well as relays assigned to CC Entr Key Rly and **P## RlyResp Type**.

P## Disp as Dvc

Default:	No
Selection:	Yes or No
Yes	Display CHECK DEVICE when this point is off-normal.
No	Do not display CHECK DEVICE when this point is off-normal.

Use **P## Disp as Dvc** to cause the keypad to display CHECK DEVICE when a point is off-normal or is acknowledged after going into alarm.



Use this function for devices with a dry contact output that faults a point when the device is in a trouble condition.

P## Local While Disarmed

Default:	Refer to the program record sheet
Selection:	Yes or No
Yes	Suppress Alarm, Trouble and Restoral* Reports from this point while the area to which it is assigned is disarmed.
No	Send event reports occurring from this point while the area is disarmed.

* Transmission of Restoral Reports continues if the alarm, trouble, or bypass (by Sked, RPS, or Swinger bypass) condition occurred when the area disarmed, and the point restored.



To meet UL 864 requirements for Central Station and Remote Station applications, set this parameter to **No**.

Use this option to allow a Controlled point (**P## Type 1, 2, 3**), to report Alarms, Troubles, and Restoral Reports only when the area is armed. This prompt does not affect local annunciation.



Local While Disarmed suppresses all reports from 24-hour points. Do not use P## Type 0 for this prompt. Remember that this option works only for Disarmed points, and a Type 0 is a 24-hour Always Armed point. Instead, choose any type other than 0, and use a point response that reports an alarm, whether or not the point is armed. For instance, P## Type 1 and P## Response 9 reports an alarm on an open or a short (I) whether the area is armed or not.

Local While Disarmed affects Keyswitch points. This prompt suppresses keyswitch (troubles and restorals) and D279 (alarms, troubles, and restorals). Do not use this parameter for these applications.



Local While Armed suppresses all reports from 24-hour points. Do not use P## Type 0 for this prompt. This setting works only for disarmed points. Type 0 is a 24-hour, always armed point. Choose any Type other than 0, and use a point response that reports an alarm whether or not the point is armed. For instance, P## Type 1 and P## Response 9 reports an alarm on a trouble or a short whether or not the area is disarmed.

Local While Armed affects Keyswitch Points. This prompt suppresses keyswitch (alarms, troubles, and restorals) and D279 (opening, closing, troubles, and restorals). Do not use this parameter for controlled points that arm or disarm.

P## Local While Armed

Default: No	
Selection: Yes or No	
Yes	Suppress Alarm, Trouble and Restoral* Reports from this point while the area to which it is assigned is armed.
No	Report events occurring from this point while the area is armed.

* Transmission of Restoral Reports continues if the alarm, trouble, or bypass (by Sked, RPS, or Swinger bypass) condition occurred when the area disarmed, and the point restored.



To meet UL 864 requirements for Central Station and Remote Station applications, set this parameter to **No**.

Allows a controlled point (P## Type 1, 2, 3), to report Alarms, Troubles, and Restoral Reports only when the area is disarmed. This prompt does not affect local annunciation.

P## Disable Rst

Default: No	
Selection: Yes or No	
Yes	Enable Restoral Reports from this point.
No	Disable Restoral Reports from this point.



To meet UL 864 requirements for Central Station and Remote Station applications, set this parameter to **No**.

Use this option to disable any Restoral Reports from this point after it returns to normal from an alarm or trouble condition.

P## FA Retrnable

Default: No	
Selection: Yes or No	
Yes	This point automatically returns to the system when it restores to normal.
No	This point stays out of the system until the area is disarmed.

Use this option to allow points that were force armed out of the area to return back to the armed state when they become normal again without having to disarm the system.



Use on loading dock doors, that must remain open until loading is completed.

After the loading dock door is closed, the point detects any subsequent opening and reports an alarm.

P## BP Retrnable

Default: No

Selection: Yes or No

Yes	This point automatically returns to the system when the area is disarmed.
No	This point stays out of the system through arming and disarming cycles.

Use this option to return a point that was bypassed, force armed, or swinger bypassed back into the system when the area to which this point is assigned is disarmed. This option applies to all point types.



Set this item to **No** for Interlock points.



When the point cannot return to the system through disarming, the point must be manually unbypassed using the Unbypass?, keypad function, Sked Functions 4 and 5, or remote programming software (RPS).



For Force Armed points to remain bypassed, ensure that **P## FA Retrnable** is set to **No**.

P## Bypassable

Default: No

Selection: Yes or No

Yes	This point can be bypassed and force armed.
No	This point cannot be bypassed or force armed from the keypad or remote programming software (RPS); however, it can be force armed by automatic arming at the end of the Closing Window (refer to the A# Auto Close prompt in <i>Section 2.9.5 Open/Close Options</i> on page 43 or by a Sked programmed to arm the area.



To meet UL 864 requirements, set this parameter to **No**.

Use this option to allow this point to be bypassed or force armed.

Bypassing a 24-hour point: When a 24-hour point or 24-hour Supervisory point is bypassed, 24 HOUR BYPASS scrolls continuously at the keypad.

Bypassing a Fire Point: FIRE BYPASS scrolls to indicate that a 24-hour Fire point or a Fire Supervisory point is bypassed.



Alternative to a 24-hour Point: For alarm capability of a 24-hour point without the continuous scrolling, use a Perimeter point with a Point Response of 9 to E.



If the P## Bypassable option is set to Yes, a point can be bypassed in several ways. Refer to *Table 31*.

Table 31: Bypassing a Point

Bypass with:	Report sent:
Keypad using the Bypass? function	Command Bypass
Keypad using Command 0	Command Bypass
Sked Function 3	Sked Bypass
Remote programming software (RPS)	RPS Bypass ¹
¹ RPS Bypass is sent at the end of the RPS session.	



If the P## Swinger Bypas option is set to Yes, a point is automatically bypassed after the fourth alarm or trouble report is sent. A Swinger Bypass report is sent at the same time.



Programming **Bypassable** as **Yes** for Cross Points can cause missed Cross-Point alarms. For example, if Points 1 and 2 were programmed as Cross Points and Point 1 was Bypassed or Force Armed, Point 2 cannot generate an Alarm Cross Point Event. Point 2 can; however, generate an Unverified or Alarm Event depending on how the point was faulted. Be careful when using this feature with Cross Point applications.

P## Swinger Byps

Default:	No
Selection:	Yes or No
Yes	Enable Swinger Bypass for this point.
No	Disable Swinger Bypass for this point.



To meet UL requirements, set this parameter to **No**.

Use the **P## Swinger Byps** parameter to allow the control panel to bypass automatically a point that reports two or more alarm or trouble events within the same arm cycle. The maximum number of faults allowed on a point is set in the **Swinger Count** prompt (refer to page 141).

The control panel reports a Swinger Bypass when the Swinger Count is reached and **P## Report Bypass at Occurrence** is set to **Yes**. If the point has a partial count (less than the Swinger Count number of events during an hour), the count is reset to zero.



P## Bypassable does not need to be programmed as **Yes** for swinger bypass to work.



A Swinger Shunted point returns to the system if **P## BP Returnable?** is **Yes**. If not, return the point to the system through manual unbyypass or [COMMAND][0][0]. Refer to **P## BP Retrnable** in the program entry guide for additional information.

P## Report Bypass at Occurrence

Default:	No
Selection:	Yes or No
Yes	Send a Command Bypass Report when the point is bypassed.
No	Do not send a Command Bypass Report when the point is bypassed.

Send a Command Bypass Report as soon as a user bypasses the point from the keypad. Enable this option for all Bypassable 24-hour points. You can also report a bypassed point at the time the area is armed. Refer to **P## Defer BP Report** on page 99.

P## Defer BP Report

Default:	No
Selection:	Yes or No
Yes	Send a Point Bypass Report with the Closing Report instead of a Command Bypass Report when a user bypasses the point.
No	Do not defer Bypass Reports.

Use this option to prevent **P## Type** (0 to F) points that are bypassed by the user (COMMAND BYPASS) from occurring until the area is armed. When the area is armed, the bypassed points and any point being bypassed during the arming sequence report as POINT BYPASS along with the Closing Report.



When **P## Defer BP Report** is set to **Yes** and Closing Reports are suppressed by using **Closing Windows**, the deferred Bypass Reports are not sent.

Bypass Reports for 24-hour points do not report if **P## Report Bypass at Occurrence** and **P## Defer Bypass Report** are both set to **No**.



To report the bypass at occurrence and when the area is armed, program **P## Report Bypass at Occurrence** and **P## Defer Bypass Report** as **Yes**. A Command Bypass Report is sent as soon as the user manually bypasses a point, and a supplemental Point Bypass Report is sent with the Closing Report.

P## Cross Point

Default:	No
Selection:	Yes or No
Yes	This point is a Cross Point.
No	This point is not a Cross Point.



Do not use Cross points for Fire points.

The **P## Cross Point** option is designed to reduce false alarms. To achieve this, program two or more points within a Cross Point Group with this prompt enabled. The Cross point feature is available only on points where **P## Pt Response** is set to a value that generates an instant alarm response.

The Cross Point feature does not activate when a fault occurs on Controlled points (Point Types 1, 2 and 3) in the disarmed, entry delay, or exit delay states. Refer to *Section 6.9 Cross Point Parameters* on page 142 for additional programming requirements to program the Cross Point Timer.

If an abort window delay is needed for the cross zone alarms, all cross zone points in the group must have **P## Alarm Abort** (refer to page 101) set to **Yes**.



The Cross Point function applies only to Instant Alarm conditions. It does not apply to Trouble or Supervisory conditions.

Cross zones have the ability to individually protect the intended area (e.g. motion detectors, which overlap).

For SIA CP-01 Compliance:

P## Cross Point can be set to **Yes** or **No**.

P## Fire Point

Default: No
Selection: Yes or No

Yes	This point is a Fire point.
No	This point is not a Fire point.



To meet UL 864 requirements, set this parameter to **Yes** for all applicable Fire points.

Use this option to make a 24-hour point a Fire point. This option makes this point the highest priority event in the control panel when an alarm occurs for both reporting and displaying on the keypad. Refer to *Section 4.2.2 Characteristics of a Fire Point* on page 91.



You should dedicate a fire annunciation device to all your Fire points if they are assigned to a single area in a multiple area system. Special red keypads and annunciators with specific keys for fire systems are designed for this type of application (D1256RB and D1257RB).



Do not use the Cross point function for Fire points.

P## Alarm Verify

Default: Refer to the program record sheet
Selection: Yes or No

Yes	Enable alarm verification on this point. Alarm verification points must be programmed as resettable.
No	Disable alarm verification on this point.

Use this option only with Fire points to designate them for alarm verification.

When an Alarm Verification point enters into alarm, the control panel removes power to all Resettable points for the duration programmed in **A# Verify Time** in *Section 2.9 Area Parameters* on page 36. If the point (or another Resettable point in the area) is still faulted, or returns to a faulted state within 60 sec after the initial verification time reset, an alarm is generated.



During a Fire Walk Test the reset time is 5 sec. The time programmed in **A# Verify Time** is ignored.

P## Resettable

Default: Refer to the program record sheet
Selection: Yes or No

Yes	This point is reset by the Reset Sensor? function and during the alarm verification sequence.
No	This point is not resettable.



To meet UL 864 requirements, set this parameter to **Yes** for applicable resettable points.

Use this option if this is a Powered point that requires interruption of power to reset a latched alarm condition. The Resettable point option is typically used with smoke detectors and glass break detectors.

When initiated (either through a Fire Walk Test or the keypad's Reset Sensor? function) or when the remote programming software (RPS) interrupts power to the device for 5 sec, a Sensor Reset report is sent to the central station receiver.



When a sensor reset occurs, the control panel does not accept alarms from any points with **P## Resettable** programmed as **Yes**. During the 5-sec reset time, alarms from these points are ignored.

Do not mix fire and intrusion devices on the same powered loop.

P## Alarm Abort

Default:	Yes
Selection:	Yes or No
Yes	If the point goes into an alarm condition, the system delays the alarm report for the amount of time specified in the control panel-wide parameter Abort Window .
No	If the point goes into an alarm condition, alarm reports are sent immediately.

This parameter allows points with the associated Point Index to delay a Burglar Alarm (non-fire) event for the time period specified in the Abort Window. An alarm is aborted by performing an alarm silence operation at a keypad showing the burglar alarm condition before this time elapses.

When an alarm is successfully aborted, the keypad shows an optional ALARM NOT SENT message and no event is sent or written in the control panel event log. Refer to **CC# Abort Display** on page 56.

For SIA CP-01 Compliance:

P## Alarm Abort can be set to **Yes** or **No**.




This feature does not apply to Fire Alarms or invisible point alarms.

4.3 Point Assignments

These entries assign point indexes to Points 1 to 127, 129 to 247 for the D9412GV3 and Points 1 to 75 for the D7412GV3, and assign the points to the areas. Also included in this section are parameters used to set the point's debounce count, Relay (for assigning relays to follow alarms for a group of points), and custom keypad and report text for each point.

Point Number

Default:	1
Selection:	1 to 127, 129 to 247
Enter the point number you are programming. When transmitting in Modem IIIa ² , the three-digit point number is reported to the D6500 or D6600.	
	Point number 128 is reserved for supervising Zonex 1.
	Point number 248 is reserved for supervising Zonex 2.

P### Point Index

Default:	Refer to the program record sheet
Selection:	Blank (00) to 31

This entry selects one of the 31 **P## Index** codes that define the point's characteristics and determines how the control panel responds to various point conditions.

Blank (00) disables the point.

Missing Point Report

If a Point Index is assigned to a point that has an incorrect address or that is not connected to the point bus, a Missing Point Report occurs.

When a POPIT is missing, the control panel generates the following responses based on the point type:

- Fire points generate missing trouble responses.
- Non-fire 24-hour points generate missing alarm responses.
- Non-fire, non 24-hour points generate missing alarm responses while armed, and trouble responses while disarmed. Exception: Non-fire, non-24-hour points with a point response of 9 to D generate a missing alarm response while disarmed.

POPIT modules monitor their sensor loops for three conditions: loop normal, loop open, and loop shorted. They send reports on these three conditions to the control panel. The control panel uses point programming to interpret the sensor loop information sent by the POPITs and to make the appropriate system response.

P### Area Assign

Default: 1
Selection: 1 to 8

The areas are numbered 1 to 8. Select the area number to which the point is assigned.

P### Debounce

Default: 2
Selection 1 to 15
 :

1	.300 sec
2	.600 sec
3	.900 sec
4	1.2 sec
5	1.5 sec
6	1.8 sec
7	2.1 sec
8	2.4 sec
9	2.7 sec
10	3.0 sec
11	3.3 sec
12	3.6 sec
13	3.9 sec
14	4.2 sec
15	4.5 sec

The debounce count is the number of times the control panel scans a point before generating an alarm. Scan cycles are 300 ms.

For appropriate settings consult the manufacturer's instructions for the device connected to this point.



Use an entry of two or higher. Interior Follower points need a Debounce value of at least three.



Door points assigned to D9210B modules need a Debounce value of at least four.

P### BFSK/Relay

Default: Refer to the program record sheet
Selection: 0 to 9



The BFSK function of this prompt is not supported.

Use this option to activate a relay when the point is faulted. Refer to *Table 32*.



BFSK/Relays do not activate for Fire Supervisory or Non-Fire Supervisory points.

Table 32: P### BFSK/Relay Codes/Relays

Relay Code	Faults Relay	
	D8129 on Zonex Bus 2 for D9412GV3*	D8129 on Zonex Bus 1 for D7412GV3*
1	73	9
2	74	10
3	75	11
4	76	12
5	77	13
6	78	14
7	79	15
8	80	16

* Address setting = 1 (on), 2 (off), 3 (on), 4 (on)



Do not assign a relay to Invisible points. To avoid activating one of the associated relays, program this prompt as 0.



Two relays can activate when this point enters into alarm if the **P## Rly Resp Type** for this point is programmed.

Use these codes to activate relays on the D8129 OctoRelay (or C8137 Transmitter Interface). You can assign the same code to several points providing a summary zone alarm output. When the point enters into alarm, the relay activates. When the alarm is acknowledged and is no longer scrolling in the keypad display, the relay resets.

P### Point Text

Default: Refer to the program record sheet
Selection: Up to sixteen alphanumeric characters

Enter alphabetic characters (A to Z) in capital letters.

Enter up to sixteen characters of text to describe the point. This point text is shown at keypads, if the point is programmed as visible, and sent to the D6500 or D6600 when transmitting in Modem IIIa² format (if it is a reporting point).

Include the point number in custom point text. This helps the user when viewing events, creating bypasses, and so on. It can also simplify troubleshooting.



When a D1260 Keypad is installed on the system, the point text for Points 240 to 247 can be used for Area Name Text for Areas 1 to 8, respectively. Refer to *Table 33*:

Table 33: Point Text for Points 240 to 247

Point Text	Corresponding Area Name Text
Point 240	Area 1
Point 241	Area 2
Point 242	Area 3
Point 243	Area 4
Point 244	Area 5
Point 245	Area 6
Point 246	Area 7
Point 247	Area 8

4.4 COMMAND 7 and COMMAND 9

These entries assign point indexes, associated relays that activate, and the text for the COMMAND 7 and COMMAND 9 keypad functions.

CMD7 Point Index

Default: 31
Selection: Blank (00) to 31

This entry selects one of the 31 **P## Index** codes that define how the control panel reacts when a COMMAND 7 is initiated.



The point index code used for COMMAND 7 must not be used for any other points on the system.



If the point index for COMMAND 7 has Fire points programmed as **Yes**, this causes access control doors to unlock if Fire Unlock is also programmed as **Yes**. Refer to the *D9210B Program Entry Guide* (P/N: 32207).

CMD7 BFSK/Relay

Default: 1
Selection: 0 to 9

This entry selects a relay (73 to 80 for the D9412GV3 or 9 to 16 for the D7412GV3) when COMMAND 7 is initiated (refer to the **P### BFSK/Relay** prompt on page 102 for relay number association). The BFSK function of this prompt is not supported in the D9412GV3 and D7412GV3 control panels.



COMMAND 7 does not activate the Summary Fire Alarm relay.

CMD7 Point Text

Default: [COMMAND][7]
Selection: Up to sixteen alphanumeric characters

Enter alphabetic characters A to Z in capital letters

Enter up to sixteen characters of text to describe the point. This point text appears at keypads (if the point is programmed as visible) and sent to the D6500 or D6600 when transmitting in Modem IIIa² format (if it is a reporting point).

CMD9 Point Index**Default:** 31**Selection:** Blank (00) to 31

This entry selects one of the 31 **P## Index** codes that define how the control panel reacts when a COMMAND 9 is initiated.



The point index code used for COMMAND 7 and COMMAND 9 must not be used for any other points on the system.



If the point index for COMMAND 9 has Fire points programmed as **Yes**, this causes access control doors to unlock if Fire Unlock is also programmed as **Yes**. Refer to the *D9210B Program Entry Guide* (P/N: 32207).

CMD9 BFSK/Relay**Default:** 1**Selection:** 0 to 9

This entry selects a relay (73 to 80 on the D9412GV3 or 9 to 16 on the D7412GV3) when COMMAND 9 is initiated (refer to the **P### BFSK/Relay** prompt on page 102 for relay number association). The BFSK function of this prompt is not supported.



COMMAND 9 does not activate the Summary Fire Alarm relay.

CMD9 Point Text**Default:** [COMMAND][9]**Selection:** Up to sixteen alphanumeric characters

Enter alphabetic characters (A to Z) in capital letters

Enter up to sixteen characters of text to describe the point. This point text is displayed at keypads (if the point is programmed as visible) and sent to the D6500 or D6600 when transmitting in Modem IIIa² format (if it is a reporting point).

5.0 RADXSKED

5.1 Windows

Use this programming module to define the windows for Opening and Closing and User Access.

5.1.1 Opening and Closing

Use these windows to set a schedule for disarming and arming. The disarming and arming schedules have several independent features:

- Suppress normal Opening or Closing Reports when **A# Disable O/C in Windows** is programmed as **Yes**.
- Generate a Fail to Open Report if the area is not disarmed on schedule when **A# Fail To Open** is programmed as **Yes**.
- Provide a warning tone and a PLEASE CLOSE NOW display at the keypad when it is time to arm the area.
- Generate a Fail to Close Report if the area is not armed on schedule when **A# Fail To Close** is programmed as **Yes**.
- Automatically arm the area at the end of the Closing Window when **A# Auto Close** is programmed as **Yes**.

Opening and closing schedules can be set up independently. For example, if you want to use features provided only by Closing Windows, leave times blank in the Opening Windows prompts and program Closing Window times.

A worksheet is provided at the end of this section for your convenience. Following the worksheet are examples of programming Opening and Closing Windows for particular applications (refer to *Table 38* on page 111 through *Table 42* on page 112).

About the program record sheet: A column labeled Sked # is found in the program record sheet provided with the control panel. The numbers in that column appear in D6500 and D6600 reports and local printer reports when the window Begin Time executes.

Window selections 1 through 8 correspond with odd-numbered Skeds 41 through 55 for Open Window and correspond with even numbered Skeds 42 through 56 for Close Window. For example, when the Opening Window for Window 1 executes, a Sked 41 Executed event is generated. Refer to *Table 34*.

Table 34: Window Selections

Selection	Sked #	Window	Sked #	Window
1	41	Open	42	Close
2	43	Open	44	Close
3	45	Open	46	Close
4	47	Open	48	Close
5	49	Open	50	Close
6	51	Open	52	Close
7	53	Open	54	Close
8	55	Open	56	Close

Window

Default: 1
Selection: 1 to 8

Enter the window number you want to program.

W# Sunday

Default:	No
Selection:	Yes or No
Yes	Activate this window on Sundays.
No	Do not activate this window on Sundays.

This prompt and the next six day-of-the-week prompts select the days of the week the Opening and Closing windows are active.

Exceptions:

To prevent the windows from activating on certain days of the year, program **Xept Holiday** as **Yes**, and enable at least one Holiday Index. When **Xept Holiday** is **Yes**, the window executes on the days of the week programmed unless the Holiday Index designates the date as a holiday.

If Opening and Closing Windows are only needed on certain days of the year, do not program the windows to execute on any days of the week. Instead, program **Xept Holiday** as **No** and select a Holiday Index with the days of the year you want the window to be active.

W# Monday

Default: No
Selection: Yes or No

W# Tuesday

Default: No
Selection: Yes or No

W# Wednesday

Default: No
Selection: Yes or No

W# Thursday

Default: No
Selection: Yes or No

W# Friday

Default: No
Selection: Yes or No

W# Saturday

Default: No
Selection: Yes or No

W# Open Early Begin

Default: 00:00
Selection: HH:MM (hours and minutes)
 00:00 to 23:59

Open Early Begin: This program item is one of three required to create an Opening Window. To finish programming an Opening Window, Open Window Start and Open Window Stop must be programmed.

The time programmed in the **W# Open Early Begin** field is the earliest time that the user is allowed to open an area before the Opening Window Start time. If Opening and Closing Reports are enabled, disarming the area between midnight and the open Early Begin time generates an Opening Report.

- If **A# Disable O/C in Window** is set to **Yes** and the area is disarmed between the Open Early Begin time and the Open Window Start time, the Opening event is sent with an Early to Open modifier. If the Open Early Begin time is the same as the Open Window Start time, no Opening Event is sent.

- If **Disable O/C in Window** is set to **No** and the area is disarmed at any time, an Opening Event is sent without an Early to Open or Late to Open modifier.

Disarming the area between the Open Window Start and open Window Stop times creates a local event in the control panel event log, but does not send the Opening Report to the central station.

Disarming the area between the Open Window Stop time and before the next window's Open Early Begin time (or midnight, whichever is earlier) generates an Opening Event with a Late to Open modifier.

When configuring multiple windows to operate on the same day, ensure that they are added to the system in chronological order. For example, if three windows are programmed to execute on Tuesday, Window 1 (W1) must occur before Window 2 (W2), and Window 2 must occur before Window 3 (W3).



Avoid programming the Open Early Begin time before a time that is between another window's Open Window Start and Open Window Stop times.



Do **not** program a window to cross the midnight boundary.

Disabled windows have a blank beginning time. If the entry for this prompt is blank, but times are programmed for Open Window Start and Open Window Stop, the window is disabled.

To disable the window, all hours and minutes spaces must be blank.



Make time entries using a 24-hour clock. For example:

Midnight is entered as 00:00
 7:00 AM is entered as 07:00
 2:45 PM is entered as 14:45
 11:59 PM is entered as 23:59

Reboot the control panel to activate today's window, if the window needs to activate on the same day you program it.

W# Open Window Start**Default:** 00: 00**Selection:** HH:MM (hours and minutes)

Enter the time you want the control panel to start the Opening Window. The window goes into effect at the beginning of the minute.



Make time entries using a 24-hour clock. For example:

Midnight is entered as 00:00
7:00 AM is entered as 07:00
2:45 PM is entered as 14:45
11:59 PM is entered as 23:59

This program item is one of three required to create an Opening Window. To program an Opening Window, Open Early Begin and Open Window Stop must also be programmed. Refer to the **W# Open Early Begin** prompt on page 106 for explanations of report features.

W# Open Window Stop**Default:** 00: 00**Selection:** HH:MM (hours and minutes)

Enter the time you want the control panel to end the Opening Window. The window stops at the end of the minute.



Make time entries using a 24-hour clock. For example:

Midnight is entered as 00:00
7:00 AM is entered as 07:00
2:45 PM is entered as 14:45
11:59 PM is entered as 23:59

This program item is one of three required to create an Opening Window. To program an Opening Window, Open Early Begin and Open Window Start must also be programmed.

If the area is not disarmed by the time the Open Window Stop time expires, the control panel generates a Fail to Open Report if **A# Fail to Open** is enabled in Area-Wide Parameters.

Opening Reports generated between the Open Window Start time and Open Window Stop time can be suppressed by programming **A# Disable O/C in Window** as **Yes**. Refer to the **W# Open Early Begin** prompt on page 106 for additional explanations of report features.



Do not use a time of 23:59 as a window stop time unless another window begins on the next day at 00:00.

Fail to Open Reports are not sent for windows that stop at 23:59.

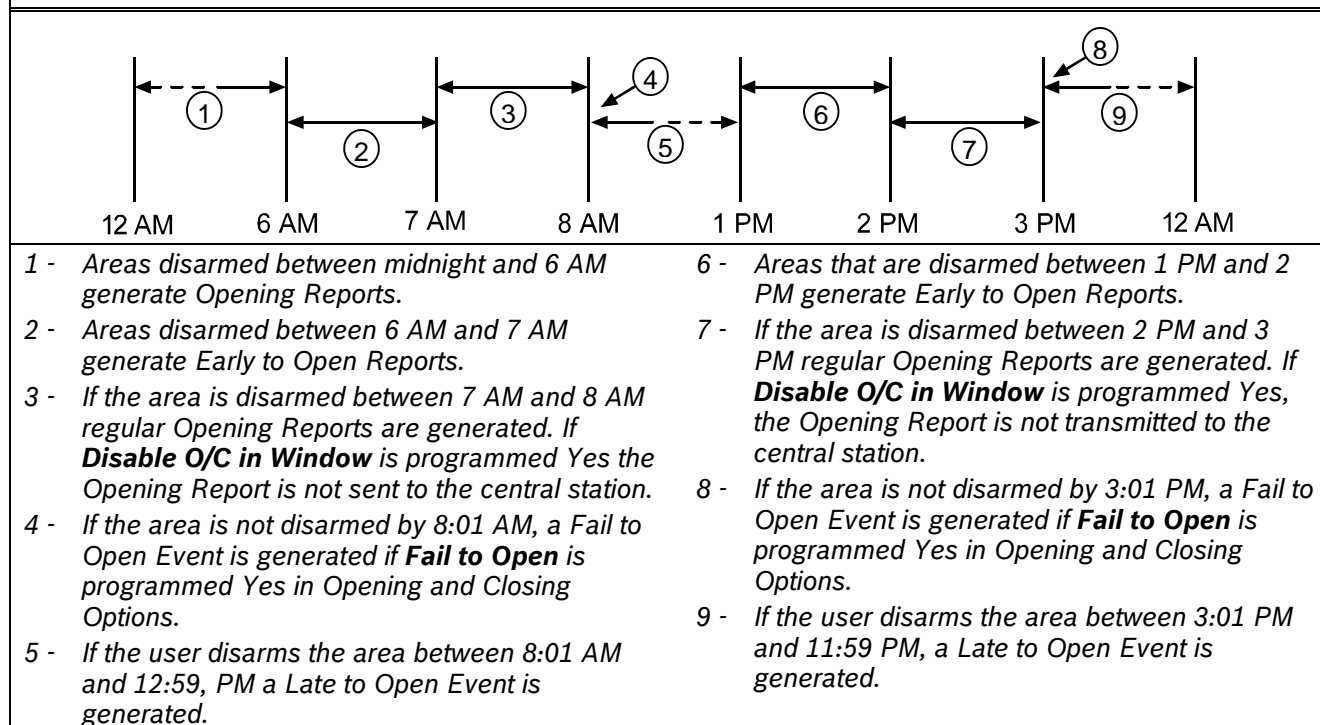
Figure 5: Example Opening Window Timeline (using two Opening Windows on same day)

Table 35: Programming for Two Same Day Opening Windows (refer to Figure 5)

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
1	S <u>M</u> T W T F S	06:00	07:00	08:00				Yes / <u>No</u>	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
2	S <u>M</u> T W T F S	13:00	14:00	15:00				Yes / <u>No</u>	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8

Do not program a single window to cross the midnight boundary. The window stop time must be later than the window start time. To program a window that effectively crosses the midnight boundary, you must program two windows.

For example, to program windows for an area that opens between 11:30 PM and 12:30 AM, five days a week, use two windows as shown in Table 36.

Table 36: Programming to Link Two Days over Midnight*

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
1	S <u>M</u> <u>T</u> <u>W</u> <u>T</u> <u>F</u> S	22:00	23:30	23:59				Yes <u>No</u>	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
2	S <u>M</u> <u>T</u> <u>W</u> <u>T</u> <u>F</u> S	00:00	00:00	00:30				Yes <u>No</u>	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8

* The setting for midnight is 00:00.

W# Close Early Begin

Default: 00:00
Selection: HH:MM (hours and minutes)
 00:00 to 23:59

Close Early Begin: This program item is one of three required to create a Closing Window. To finish programming a Closing Window, Close Window Start and Close Window Stop must be programmed.

The time programmed in the Close Early Begin field is the earliest time the user can close an area before the Closing Window Start time. If Opening and Closing Reports are enabled, arming the area between midnight and the Close Early Begin time generates a Closing Report. Additionally:

- If **A# Disable O/C in Window** is set to **Yes** and the area is armed between the Close Early Begin time and the Close Window Start time, the Closing Event is sent with an Early to Close modifier. If the Close Early Begin time is the same as the Close Window Start time, no Closing Event is sent.
- If **A# Disable O/C in Window** is set to **No** and the area is armed at any time, a Closing Event is

sent without the Early to Close or late to Close modifiers.

Arming the area between the Close Window Start and Close Window Stop times creates a local event in the control panel event log, but does not send the Closing Report to the central station.

Arming the area after the Close Window Stop time and before the next window's Close Early Begin time (or midnight, whichever is earlier) generates a Closing Event with a Late to Close modifier.

When configuring multiple windows to operate on the same day, ensure that they are added to the system in chronological order. For example, if three windows are programmed to execute on Tuesday, Window 1 (W1) must occur before Window 2 (W2), and Window 2 must occur before Window 3 (W3).



Avoid programming the Open Early Begin time before a time that is between another window's Open Window Start and Open Window Stop times.

Disabled windows have a blank beginning time. If the entry for this prompt is blank, but times are programmed for Close Window Start and Close Window Stop, the window is disabled.

To disable the window, both the hours and minutes spaces must be blank.

00:00 is midnight, 23:59 is 11:59 PM. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

If the window must activate on the same day as it is programmed, reboot the control panel to activate the window immediately.

W# Close Window Start

Default: 00: 00
Selection: HH:MM (hours and minutes)

Enter the time that you want the control panel to start the Closing Window. The window goes into effect at the beginning of the minute.

00:00 is midnight, 23:59 is 11:59 PM. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

This program item is one of three required to create a Closing Window. To program a Closing Window, Close Early Begin and Close Window Stop must also be programmed.

If the area is not armed when the Close Window Start time comes, a warning tone sounds and PLEASE CLOSE NOW appears at the keypad. To temporarily silence the tone, press the [ESC] key on the keypad. The warning tone restarts in 10 min if the area is not armed.

Refer to the **W# Close Early Begin** prompt in this section for explanations of report features.

W# Close Window Stop

Default: 00: 00
Selection: HH:MM (hours and minutes)

Enter the time that you want the control panel to end the Closing Window. The window stops at the end of the minute.

00:00 is midnight, 23:59 is 11:59 PM. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

This program item is one of three required to create a Closing Window. To program a Closing Window, Close Early Begin and Close Window Stop must also be programmed.

If the area is not armed by the time the Close Window Stop time expires, the control panel generates a Fail to Close Report if enabled in Fail To Close.

Closing Reports generated between the Close Window Start time and Close Window Stop time can be suppressed by programming **Disable O/C in Window** as **Yes**. Refer to the **W# Close Early Begin** prompt for other explanations of report features.

Do not use a time of 23:59 as a window stop time unless the window continues on the next day at 00:00. Fail to Close Reports are not sent, and the Auto Close feature does not work for windows that stop at 23:59.

Do not program a single window to cross the midnight boundary. The window stop time must be later than the window start time. To program a window that effectively crosses the midnight boundary, you must program two windows.

For example, to program windows for an area that closes between 11:30 PM and 12:30 AM, five days a week, use two windows as shown in *Table 37*.

Table 37: Programming Example: Linking Two Closing Windows over Midnight

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
1	S M T W T F S				22 : 00	23 : 30	23 : 59	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
2	S M T W T F S				00 : 00	00 : 00	00 : 30	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8

W# Xept Holiday

Default: No	
Selection: Yes or No	
Yes	Do not activate this window on holidays. To use this selection, the window must be programmed to activate on at least one day of the week and a Holiday Index must be enabled.
No	A holiday does not prevent this window from activating. You also use this selection if Opening or Closing Windows are needed only on certain days of the year. Do not program the windows to execute on any days of the week. Instead, program Xept Holiday as No , and select at least one Holiday Index with the days of the year you want the window to be active.

Determine if the window is disabled on holidays, or is active only on holidays.

To prevent the windows from activating on certain days of the year, program **Xept Holiday** as **Yes**, and enable at least one Holiday Index. When **Xept Holiday** is programmed as **Yes**, the window executes on the days of the week programmed unless the date is designated as a Holiday by the Holiday Index(es) selected.

Holiday Indexes for O/C Windows

You can enable up to four Holiday Indexes for use with Opening/Closing Windows. Enable at least one Holiday Index if **W# Xept Holiday** is programmed as **Yes** for this window, or if you want this window to activate only on specific dates. Holidays are programmed in *Section 5.3 Holiday Indexes* on page 123.

W# Holiday 1

Default: No	
Selection: Yes or No	
Yes	Use Holiday Index 1 with this window.
No	Do not use Holiday Index 1 with this window.

W# Holiday 2

Default: No	
Selection: Yes or No	
Yes	Use Holiday Index 2 with this window.
No	Do not use Holiday Index 2 with this window.

W# Holiday 3

Default: No	
Selection: Yes or No	
Yes	Use Holiday Index 3 with this window.
No	Do not use Holiday Index 3 with this window.

W# Holiday 4

Default: No	
Selection: Yes or No	
Yes	Use Holiday Index 4 with this window.
No	Do not use Holiday Index 4 with this window.

W# Area 1 [through 8]

Default: No	
Selection: Yes or No	
Yes	Activate the window in the area number (#) specified.
No	Disable the window in the area number (#) specified.

Eight separate program items determine whether a particular window activates in each of the eight areas of the control panel.

Table 38: Opening and Closing Windows Worksheet

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
1	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
2	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
3	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
4	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
5	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
6	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
7	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
8	S M T W T F S	--:--	--:--	--:--	--:--	--:--	--:--	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8

Table 39: Opening and Closing Windows

The column below briefly describes how to activate an Opening—Closing Window. Use the guidelines shown in the other columns to choose the appropriate entries.					
Day of Week		eXcept On Holiday	Holiday Index	Areas	
Program at least one day Yes .	Day(s) of the week	No	None	Program at least one area Yes .	
Program at least one day Yes .	Day(s) of the week, but not on holidays	Yes	Select at least one Index	Program at least one area Yes .	
Program at least one day Yes .	Day(s) of the Week, plus holidays	No	Select at least one Index	Program at least one area Yes .	
All days must be programmed No .	Only on holidays	No	Select at least one Index	Program at least one area Yes .	

Table 40: Normal Store Hours*

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
1	S <u>M T W T F</u> S	04:00	05:00	06:00	20:00	23:00	23:59	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
2	S M <u>T W T F</u> S	--:--	--:--	--:--	00:00	00:00	01:00	Yes No	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8

* Monday to Friday, Opening between 5 AM and 6 AM. Closing between 11 PM and 1 AM.

Table 41: Delivery Schedule*

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
3	S <u>M</u> T <u>W</u> T F S	02 : 30	02 : 45	03 : 00	03 : 05	03: 15	03: 30	<u>Yes</u> No	<u>1</u> 2 3 4	<u>1</u> 2 3 4 5 6 7 8
						00 : 00	01 : 00	Yes <u>No</u>	1 2 3 4	<u>1</u> 2 3 4 5 6 7 8
	Program at least one day Yes .	Day(s) of the week, but not on holidays						Yes	Select at least one index	Program at least one area Yes .

* Monday and Wednesday, In between 2:45 AM and 3:00 AM. Out between 3:15 AM and 3:30 AM.

Another alternative for delivery schedules is to automatically bypass specific points using skeds.

Table 42: Monthly Auditor's Schedule*

W#	Day of Week	Open			Close			eXcept On Holiday	Holiday Index	Area(s)
		Early Begin	Start	Stop	Early Begin	Start	Stop			
4	S M T W T F S	07 : 00	08 : 00	08 : 30	14 : 00	14: 30	17: 00	Yes <u>No</u>	1 <u>2</u> 3 4	<u>1</u> 2 3 4 5 6 7 8
	All days must be programmed No .	Only on holidays						No	Select at least one index	Program at least one area Yes .

* Sunday, In between 8:00 AM and 8:30 AM. Out between 2:30 PM and 5:00 PM..

5.1.2 User Group Windows

In this section, you can create up to eight User Group periods where the passcodes for the group chosen is enabled. One user group can have multiple windows assigned to it over a 24-hour period. Refer to the **U### User Group** prompt in *Section 3.1 Passcode or Token Worksheet* to assign individuals to a group.

When you assign a **U### User Group** to one of the eight windows, all passcodes for the group are enabled **ONLY** for the period between the Enable Time and Disable Time for assigned **User Windows #**.

If a user is not assigned to a **U### User Group** or the number programmed for the user for **U### User Group** is not assigned to a **User Windows #**, the passcode for that user is enabled all the time.



User Group Windows **do not** affect the users token or card access authority. To enable/disable tokens, the Sked Function Access Levels On/Off must be used.

User Windows

Default: 1

Selection: 1 to 8

Enter the User Windows number you want to program.

UW# User Group

Default: 1

Selection: Blank, 1 to 8

Enter the number programmed for the group of users in the **U### User Group** prompt. This group has its user passcodes enabled or disabled when this window runs.



A User Group can be assigned to more than one window in a 24-hour period, but the windows must not overlap or exceed the midnight boundary.

UW# Sunday

Default: No
Selection: Yes or No

This prompt, and the next six day of the week prompts, select the days of the week that the User Group Window is active.



Refer to the **W# Sunday** prompt in *Section 5.1.1 Opening and Closing* on page 105 for more information about programming this prompt.

UW# Monday

Default: No
Selection: Yes or No

UW# Tuesday

Default: No
Selection: Yes or No

UW# Wednesday

Default: No
Selection: Yes or No

UW# Thursday

Default: No
Selection: Yes or No

UW# Friday

Default: No
Selection: Yes or No

UW# Saturday

Default: No
Selection: Yes or No

UW# Group Enable

Default: 00:00
Selection: HH:MM (hours and minutes)



This prompt must be programmed if this User Group Window is assigned to a user group.

Enter the time of day when the window starts. Beginning at this time, users assigned to this window's group can use their passcodes. The window goes into effect at the beginning of the minute. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

If the window must activate on the same day that you program it, reboot the control panel to activate it immediately.

UW# Group Disable

Default: 00:00
Selection: HH:MM (hours and minutes)



This prompt must be programmed if this User Group Window is assigned to a user group.

Enter the time of day when the window ends. This time marks the end of the period in which users assigned to this window's group can use their passcodes. The window stops at the end of the minute. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

To disable the window, both the hours and minutes spaces must be blank.

Do not program a single window to cross the midnight boundary. The window stop time must be later than the window start time.

5.1.3 Holiday Indexes for User Group Windows

You can enable up to four Holiday Indexes to use with User Group Windows. Enable at least one Holiday Index if **UW# Xept Holiday** is programmed as **Yes** for this user window, or if you want this window to activate only on specific dates. Holidays are programmed in Holiday Indexes. Refer to *Section 5.3 Holiday Indexes* on page 123 for programming information.

UW# Xept Holiday

Default: No
Selection: Yes or No

Determine if the window is disabled on holidays, or is active only on holidays. Use the instructions provided in the **W# Xept Holiday** prompt on page 110.

UW# Holiday 1 [through 4]

Default: No
Selection: Yes or No

Yes	The selected holiday index can be used by users in the User Group window.
No	The selected holiday index does not apply to users in this User Group.

5.2 Skeds

Use the Skeds module to program the control panel to automatically execute functions that are otherwise started by the end user at the keypad. Each sked can be programmed to occur at a specific time on a specific date or day of the week. Up to 40 Skeds can be programmed.

A sked can be edited from the keypad if **S## Time Edit?** is **Yes**. The date and time can be changed using the Change Sked function.

Each sked number can be programmed with one of 24 functions for the **S## Function Code**. In addition to the function, a choice must be made as to what is affected by the function. For example, when choosing Function 2 (Disarm Sked), the disarming is the function and the selected areas are what is affected.

The functions and their associated parameters are listed in the Sked Function Code Table in the *D9412GV/D7412GV3 Program Record Sheet* (P/N: F01U143072), and they are explained in detail following the **S## Function Code** prompt on page 114.

Each sked can be programmed with up to four Holiday Indexes. The Holiday Indexes can execute the sked on the holidays as well as on the date or day(s) of the week, or, they can prevent the sked from executing on the holidays (refer to **S## Xept Holiday** prompt in this section).

Sked Number

Default: 1
Selection: 1 to 40

Enter the number of the sked you are programming.

S## TimeEdit

Default: Yes
Selection: Yes or No

Yes	The user can edit the time of this sked from the keypad and determines if this sked appears in the CHG SKED display.
No	The user cannot edit the time of this sked from the keypad and the sked does not appear in the CHG SKED display.

Select whether the user can edit the time of this sked from the keypad.

S## Function Code

Enter the function code you want this sked to execute. Sked Function 12 is reserved and is not a valid entry.

The D5200 Programmer automatically retrieves the appropriate sub-menu when the user enters a function code. Refer to the following examples:

- Example 1:** When Function Code 1 (Arm Area) is entered, the **S## Area 1 [through 8]** prompt appears.
- Example 2:** When Function Code 3 (Bypass a Point) is entered, the **S## Point Number** prompt appears.

After you program the parameter choices associated with the Sked function, press [EXIT GROUP] to continue programming the sked for date, day of week, time, and holiday.

Default: Blank Selection: 1 to 11, 13 to 24, 28, 29				
1	Arm Area: This function simulates the Master Arm Delay keypad function. Entries in the S## Area # prompts define the area(s) this sked arms. The sked can arm multiple areas. If any point is faulted when the sked executes, it is force armed regardless of the A# FA Bypass Max setting.	<div>S## Area 1[through 8]</div> Default: No Selections: Yes or No Enable the sked to arm the areas indicated with Yes .	Yes No	Arm Area #. Do not arm Area #.
2	Disarm Area: This function emulates the DISARM #? or DISARM ALL? keypad function list options. Entries in the S## Area # prompts define the area(s) this sked disarms. The sked can disarm multiple areas.	<div>S## Area 1[through 8]</div> Default: No Selection: Yes or No Enable the sked to disarm the areas indicated with Yes .	Yes No	Disarm Area #. Do not disarm Area #.
3	Bypass a Point: This function emulates the Bypass Pt? keypad function. The entry in the S## Point Number prompt defines the point this sked bypasses. The point can be bypassed only if Bypassable is programmed Yes in the point index assigned to the point. The bypass is reported if the Bypass Reports is enabled by the point index settings assigned to the point. The sked can bypass one point.	<div>S## Point Number</div> Default: Blank Selections: Blank, 1 to 127, 129 to 247 for D9412GV3, 1 to 75 for D7412GV3 Enter the number of the point the sked bypasses.	Blank (0) 1 to 127, 129 to 247	No point is bypassed Point to bypass
4	Unbypass a Point: This function emulates the Unbypass Pt? keypad function. The entry in the S## Point Number prompt defines the point this sked unbypasses. The sked can unbypass one point.	<div>S## Point Number</div> Default: Blank Selections: Blank, 1 to 127, 129 to 247 for D9412GV3, 1 to 75 for D7412GV3 Enter the number of the point the sked unbypasses.	Blank (0) 1 to 127, 129 to 247	No point is unbypassed. Point to unbypass.

Default: Blank				
Selection: 1 to 11, 13 to 24, 28, 29				
5	Unbypass All Points: This function is not available as a keypad function. The entry in the S## Area # prompt defines the area(s) where the sked unbypasses all points. The sked unbypasses all points in the area, regardless of how they were bypassed. This sked can unbypass all points in multiple areas.	<div>S## Area 1[through 8]</div> <p>Default: No Selection: Yes or No Select Yes to unbypass all points in the areas indicated.</p>	Yes No	Unbypass all points in Area #. Do not unbypass all points in Area #.
6	Relay On: This function emulates the Chg Relay keypad function to turn relays on. The entry in the S## Relay Number prompt defines the specific relay this sked activates. The sked can activate one relay.	<div>S## Relay Number</div> <p>Default: Blank Selections: Blank, 1 to 128 for D9412GV3, 1 to 64 for D7412GV3 Enter the number of the relay the sked activates</p>	Blank 1 to 128	No relay is activated. Relay to activate.
7	Relay Off: This function emulates the Chg Relay? keypad function to turn relays off. The entry in the S## Relay Number prompt defines the relay this sked turns off. The sked can turn off only relays that are set by a sked. The sked can turn off one relay.	<div>S## Relay Number</div> <p>Default: Blank Selections: Blank, 1 to 128 for D9412GV3, 1 to 64 for D7412GV3 Enter the number of the relay that turns the sked off.</p>	Blank 1 to 128	No relay is turned off. Relay to turn off.
8	All Relays Off: This function is not available as a keypad function. This sked function turns off all relays that are turned on by a sked. This is a panel-wide function. No other parameters require input for this option.			

Default: Blank Selection: 1 to 11, 13 to 24, 28, 29				
9	<p>Test Report: This function emulates the Test Report? sub-function of the Send Report? keypad function ([COMMAND][4][1]). This function generates a Test Report only from Area 1 but contains panel-wide status information. The report is sent to the phone(s) programmed for Test and Status Reports in <i>Section 2.3.8 Dialing Attempts</i> on page 17.</p> <p>If Expand Test Rpt in Phone parameters is programmed as Yes, the Test Report also includes all off-normal states for events listed in <i>Test Reports</i> (refer to <i>Table 14</i> on page 20) and some events listed in <i>Diagnostic Reports</i> (refer to the footnotes with <i>Table 15</i> on page 20)</p> <p>The Test Report can be deferred if any other report was sent since the last Test Report. To defer the Test Report, program S## Defer Test.</p> <p>The Test Report can be sent every hour beginning at the time scheduled in S## Time. To send a Test Report every hour, program S## Hourly Rpt.</p>	<div>S## Defer Test</div> <p>Default: No Selection: Yes or No Enable sked to defer the Test Report</p>	Yes No	Defer the Test Report. Send the Test Report on schedule.
		<div>S## Hourly Report</div> <p>Default: No Selection: Yes or No Select Yes to send the Test Report every hour.</p>	Yes No	Send the Test Report every hour. Send the Test Report only as scheduled.
10	<p>Status Report: This function generates a Status Report for each area that is enabled. The report is sent to the phone(s) programmed for Test and Status Reports in Routing.</p> <p>The Status Report can be deferred if any other report was sent since the last Status Report. To defer the Status Report, program S## Defer Status.</p>	<div>S## Defer Status</div> <p>Default: No Selection: Yes or No Enable sked to defer the Status Report.</p>	Yes No	Defer the Status Report. Send the Status Report on schedule.



To meet UL 864 requirements, use the Sked function to meet the daily **Test Report** requirement.

Default: Blank Selection: 1 to 11, 13 to 24, 28, 29				
11	Execute Custom Func: This function emulates any of the custom functions assigned to the keypad that can be executed by a user from the keypad. When a sked executes a custom function, it is subject to the scope of the selected keypad. Cmd Center and Custom Func prompts appear after entering Function Code 11. Both entries are required.	<div>S## Cmd Center</div> Default: Blank (0) Selections: Blank (0), 1 to 8 Identify the specific keypad (CC #) where the Custom Function is entered. Only one keypad can be assigned for this sked function.	Blank (0) 1 to 8	No keypad is specified for Custom Function activation. Command center (keypad) address specified for Custom Function activation.
		<div>S## Custom Func</div> Default: Blank (0) Selections: Blank (0), 128 to 143 for D9412GV3, 128 to 131 for D7412GV3 Enter the custom function this sked executes.	Blank (0) 128 to 143	No Custom Function is activated. Custom Function to activate.



Avoid having multiple functions occur at the same time at the same address. Functions can clash and the effect on the control panel is unpredictable.



Ensure that the Custom Function being executed or any of the commands nested inside the Custom Function are not passcode protected.




Do not program multiple skeds to execute at the same keypad during the same time.

Do not program skeds to execute at times when a user is likely to be executing functions at the keypad. If it is necessary to do so, there are two ways to work around the situation:

1. Program CC at the beginning of the Custom Function Key Strokes entry. This aborts the user's function and allows the sked to execute.
2. Program the sked to execute at an address (Cmd Center) with no keypad physically attached to it. The CC # must be assigned to an area and have the appropriate scope programmed.

Default: Blank Selection: 1 to 11, 13 to 24, 28, 29	
13	Adjust Time Forward One Hour: This sked function is used to make adjustments to the control panel's clock. A typical application is to program this to go into effect at 2:00 AM on the date that Daylight Saving Time begins (during the springtime). No Time Change Report is sent or logged, but the new time appears in the next report logged. No other parameters require input for this option.
14	Adjust Time Backward One Hour: This sked function is used to make adjustments to the control panel's clock. A typical application is to program this to go into effect at 2:00 AM on the date that Daylight Saving Time ends (during the fall). This function can operate only once in a day, even if multiple Skeds with this function are programmed. No Time Change Report is sent or logged, but the new time appears in the next report logged. There are no other parameters that require input for this option.

 To regulate a user's access for certain doors, assign the user a different authority level # with the same authority functions enabled. For example, a user can be assigned Authority Level 1 for Door 1 and Authority Level 2 for the remaining doors. You can enable or disable Authority Level 1 for Door 1 without affecting his authority level for Doors 2 through 8).

Default: Blank				
Selection: 1 to 11, 13 to 24, 28, 29				
19	Secure Door: This function emulates the SECURE? 12345678 keypad function for securing a door.	<div>S## Door 1 [through 8]</div> Default: No Selection: Yes or No Enable the sked to return the doors programmed Yes to the secured state.	Yes No	Secure Door #. Do not secure Door #.
20	Lock Door: This function returns an unlocked (Function 18) or secured (Function 19) door to a normal locked door state.	<div>S## Door 1 [through 8]</div> Default: No Selection: Yes or No Enable the sked to lock the doors programmed as Yes and return them to the normal Door Mode.	Yes No	Lock Door #. Do not lock Door #.
21	Access Authority Events On: The control panel can log Access Granted Events when a valid token, RTE, REX, or Unlock Door event is detected for a specific door. These events can be directed to print at a local printer or send a report remotely through phone routing. This sked enables Access Granted Events to be reported for Door #.	<div>S## Door 1 [through 8]</div> Default: No Selection: Yes or No This parameter enables the sending of Access Granted Events for Door #.	Yes No	Enable the sending of Access Granted Events for Door #. Do not enable the sending of Access Granted Events for Door #.
22	Access Authority Events Off: The control panel can log Access Granted Events when a valid token, RTE, REX, or Unlock Door Event is detected for a specific door. These events can be directed to print at a local printer or send a report remotely through phone routing. This sked disables Access Granted Events to be reported for Door #.	<div>S## Door 1 [through 8]</div> Default: No Selection: Yes or No This parameter disables the sending of Access Granted Events for Door #.	Yes No	Disable the sending of Access Granted Events for Door #. Do not disable the sending of Access Granted Events for Door #.



S## Time**Default:** 00:00**Selection:** HH:MM (hours and minutes)

Enter the time that the sked executes. Make entries using a 24-hour clock (for example, 7:00 AM is entered as 07:00, 2:45 PM is entered as 14:45).

Disabled skeds can have a blank time; however, to ensure that a sked is fully disabled, enter [COMMAND][5][2] (Change Skeds function) and select DISABLE?.

To program a time:

1. Press the two digits representing the hour.
2. The cursor advances past the colon (:) in the display.
3. Press the two digits representing the minutes.
4. Press [ENTER].

S## Date**Default:** _ _ / _ _**Selection:** MM/DD (month and date)

Enter the date that the sked executes.

Disabled skeds have a blank date. If you copy the control panel and the entry for this prompt is blank, but dates were programmed before, the sked can be disabled from the keypad using the Change Skeds function.

To program a date:

1. Press the two digits representing the hour.
2. The cursor advances past the colon (:) in the display.
3. Press the two digits representing the minutes.
4. Press [ENTER].

S## Sunday**Default:** No**Selection:** Yes or No

Yes	Activate this sked on Sundays.
No	Do not activate this sked on Sundays.

This prompt and the next six prompts select the days of the week when the sked is active.

Exceptions:

To prevent the sked from activating on certain days of the year, program **Xept Holiday** as **Yes**, and enable at least one Holiday Index. When **Xept Holiday** is programmed as **Yes**, the window executes on the days of the week programmed unless the date is designated as a holiday by the Holiday Index selected.

If a sked is only needed on certain days of the year, do not program the sked to execute on specific days of the week. Instead, program **Xept Holiday** as **No**, and select a Holiday Index with the dates you want the window to be active.



To meet UL 864 requirements for Central Station and Remote Station applications, program each day of the week to **Yes** for the required Test Report Sked.

S## Monday**Default:** No**Selection:** Yes or No**S## Tuesday****Default:** No**Selection:** Yes or No**S## Wednesday****Default:** No**Selection:** Yes or No**S## Thursday****Default:** No**Selection:** Yes or No**S## Friday****Default:** No**Selection:** Yes or No**S## Saturday****Default:** No**Selection:** Yes or No

S## Xept Holiday

Default:	No
Selection:	Yes or No
Yes	Prevent this sked from operating on the holidays identified in the specific Holiday Index(es) used with this sked. Specific Holiday Indexes are selected in this programming section and programmed in the next programming module.
No	This sked operates on holidays programmed in the Holiday Index(es) used with this sked.

If no days of the week are programmed, this sked operates only on the holidays programmed in the Holiday Index(es) used with this sked. This sked also operates if the holiday falls on a day of the week that is programmed.

S## Holiday 1

Default:	No
Selection:	Yes or No
Yes	Use Holiday Index 1 with this sked.
No	Do not use Holiday Index 1 with this sked.

S## Holiday 2

Default:	No
Selection:	Yes or No

S## Holiday 3

Default:	No
Selection:	Yes or No

S## Holiday 4

Default:	No
Selection:	Yes or No

5.3 Holiday Indexes

This programming module has two sections: Add/Change/Delete and View Holidays. Use the Add/Change/Delete section to program the Holiday Indexes. The View Holidays section is a view-only section provided for your convenience. Use View Holidays to review the dates programmed in the Holiday Indexes.

5.3.1 Add/Change/Delete

Program the dates for each of the Holiday Indexes. You can program up to four Holiday Indexes in the control panel. Within each index, you can select up to 365 dates to be designated as holidays.

The Holiday Indexes function independently of each other. The same day can be programmed in all four schedules. Holiday Indexes are used in programming O/C Windows, User Access Windows, and skeds.

Date

Default:	--/--
Selection:	MM/DD (month and date)

This entry selects the month and day you are designating as a holiday.

To program a date:

1. Press the two digits representing the month. The cursor advances past the slash (/) in the display.
2. Press the two digits representing the day of the month.
3. Press [ENTER].

To delete a date:

1. At the **Date** prompt, enter the month and day you want to delete and press [ENTER].
2. Advance to the holiday index number that you want to delete the date from. Change the entry to **No**. Press [ENTER].
If you want the date completely removed as a Holiday, it must be programmed as **No** for all of the Holiday Index # entries.

Holiday Index 1

Default:	No
Selection:	Yes or No
Yes	Use this date in Holiday Index 1.
No	Do not use this date in Holiday Index 1.

Holiday Index 2

Default: No
Selection: Yes or No

Holiday Index 3

Default: No
Selection: Yes or No

Holiday Index 4

Default: No
Selection: Yes or No

5.3.2 View Holidays

The View Holidays section is a view only section provided for your convenience. Use View Holidays to review the dates you programmed into each of the Holiday Indexes.

You can view the first 100 dates programmed in each of the indexes.

Index 1 Days

Default: Blank
Selection: Enter group or press [↓] key

Press [ENTER GROUP] to view the dates programmed in **Holiday Index 1**.

Press [↓] key to advance to the next Holiday Index.

Index 2 Days

Default: Blank
Selection: Enter group or press [↓] key

Index 3 Days

Default: Blank
Selection: Enter group or press [↓] key

Index 4 Days

Default: Blank
Selection: Enter group or press [↓] key

6.0 GV2AUX**6.1 Introduction**

The GV2AUX Handler is used primarily for programming Enhanced Communication capabilities for the GV3 Control Panels.

“Enhanced communications” represents the ability to provide new communication functions for the control panels using the SDI bus including:

- Routing control panel events to a network interface module (NIM).



A network interface module (NIM) can be a DX4020 or an ITS-DX4020-G.

- Communicating with remote programming software (RPS) using a network interface module (NIM).
- Communicating with a remote or local automatic software package.

6.2 RPS and D5200 Handler Requirements

In order to program the GV2AUX parameters for the control panels, you must use RPS version 5.12 or later and the latest handlers. To update to the latest handlers for your D5200 Programmer, call the Bosch Security Systems, Inc. Handler Update System at (800) 657-4584.

The GV2AUX handler currently has seven sections:

- SDI Automation
- SDI RPS Parameters
- Enhanced Communications
- SDI RPS/Enhanced Communication Configuration
- Miscellaneous
- Cross Point Parameters
- Route Group Rate

The handler required for these options is GV2AUX version 1.0 and above. It is available on the Handler Update System at Bosch Security Systems, Inc.

6.3 SDI Automation

SDI automation defines the characteristics of a serial interface module (SIM) when used with home or business automation software. The SIM is a two-way SDI to a serial communication module that allows the control panels to send and receive information to and from an external software program.



The SIM can be a D9133, DX4010i, or DX4020 (configured to emulate serial communication).

A DX4010i can be used only for programming.

This automation protocol allows external software programs to interact and perform functions such as:

- arming and disarming areas,
- changing user passcodes and names, and
- turning relays on and off.

The items described in this section allow some simple configuration options. To receive the SIM automation protocol; however, you must contact Bosch Security Systems, Inc. Technical Support at (888) 886-6189.

Enable SDI Auto

Default:	No
Selection:	Yes or No
Yes	Enable Automation software.
No	Disable Automation software.

Changing this item to **Yes** enables the automation address (SDI Address 80).

Baud Rate

Default:	9600
Selection:	300, 1200, 2400, 4800, 9600, 14.4 K

This item determines the baud rate between the serial interface module (SIM) and the external hardware connected to it. Since the SDI bus communicates at 9600 baud, keep this prompt at 9600 baud. Pressing the [SPACE] bar on the D5200 toggles through the available options.

Parity/Stop

Default:	No/1
Selection:	No/1, No/2, Odd/1, Even/1
No/1	No parity, 1 stop bit
No/2	No parity, 2 stop bits
Odd/1	Odd parity, 1 stop bit
Even/1	Even parity, 1 stop bit

This prompt addresses two items: parity and the number of stop bits. Pressing the [SPACE] bar on the D5200 toggles through the available options.

Supervise SDI 80

Default:	No
Selection:	Yes or No
Yes	Supervise the serial interface module (SIM).
No	Do not supervise the serial interface module (SIM).

This item determines whether the serial interface module (SIM) is supervised or not. If the SIM is supervised, disconnecting the SIM from the control panel creates a Trouble SDI 80 Event and the keypad annunciates a trouble tone (if programmed) and displays SERVC SDI 80.



Trouble SDI 80 Reports are always sent using the account number for Area 1.

RTS Control

Default:	On
Selection:	On, AutoX, Off, AutoR
On	Sets RTS to on (hardware control).
AutoX	Automatically enables Xon/Xoff (software control).
Off	Sets RTS off (hardware control).
AutoR	Sets this to Auto RTS.

This item determines how the Request To Send (RTS) Control parameters are defined for the serial interface module (SIM). Pressing the [SPACE] bar on the D5200 toggles through the available options.

DTR Control

Default:	On
Selection:	On, AutoD, Off
On	Sets DTR to on (hardware control).
AutoD	Sets this to Auto DTR.
Off	Sets DTR off (hardware control).

This item determines how the Data Terminal Ready (DTR) Control parameters are defined for the D9133. Pressing the [SPACE] bar on the D5200 toggles through the available options.

Status Rate

Default:	0
Selection:	0 to 255
0	Status information is sent only when requested.
1 to 255	Status information is sent at the interval programmed.



If the Status Rate is set to a value less than 10, and 1 to 6 SDI devices are connected to the system, the fastest the control panel can send the status information is in approximately 1 sec. If more than six SDI devices are connected to the control panel, the fastest the control panel can send the information is in approximately 1.5 sec to 2 sec.

This item determines how often the default status information is sent to the serial interface module (SIM). The status information includes:

- The current point status (normal or off-normal),
- The control panel's area status (Master Armed, Master Instant Armed, Perimeter Delay Armed, Perimeter Instant Armed, Disarmed, Area Entry Delay, Perimeter Entry Delay, Area Exit Delay, and Perimeter Exit Delay)
- The control panel status (AC Fail, Battery Missing, AC Restore, Battery Low, and so on)
- Relay status (relay on or relay off)

Entries are in 100 millisecond increments. If a 5 is entered, the status information is sent every 500 milliseconds (or 0.5 sec). An entry of 10 equals 1 sec.

6.4 SDI RPS Parameters

Configure remote programming software (RPS) parameters when communicating over a private local-area network (LAN), wide-area network (WAN), or general packet radio system (GPRS). To allow RPS to communicate with a control panel over a LAN or WAN, an SDI-Ethernet two-way network interface module (NIM) and RPS (version 3.8 or higher) are required. The computer on which RPS is installed needs a network card. See your information systems administrator for network requirements.

This section allows you to:

- Define the RPS parameters necessary to communicate by an external modem that can be connected to a D9133DC Direct Connect Programming Module.
- Provide for local programming by a DX4010i or D9133DC Serial Interface Module.
- Provide remote programming by a Conettix DX4020 Network Interface Module or an ITS-DX4020-G.
- Provide enhanced route paths for event reporting through a network using a DX4020 Network Interface Module.

Although not listed in this section, RPS checks for the RPS passcode (refer to *Section 2.7 RPS Parameters* on page 32), Datalock Code, and control panel type to determine if this RPS session should continue.



The **RPS via Phone?** prompt (Figure 6 on page 128), if selected, contacts RPS by the control panel phone line and not the external modem. Users cannot start an RPS session by the external modem. If you are using an external modem, RPS sessions can be started only by programming Answer Armed and Answer Disarmed (to a value greater than 0) or by setting **RPS Line Monitor** to **Yes** (refer to *Section 6.4.2 Using an External Modem* on page 129).

6.4.1 User Interface Modifications for COMMAND 43

COMMAND 43 can communicate with RPS by a network path. *Figure 6* on page 26 shows the structure of COMMAND 43.

Pressing the [ESC] key during the display of CONTACT RPS?, ANSWER NOW?, RPS VIA PHONE?, or RPS VIA NETWORK? exits the user to Idle Text.

Enable SDI RPS

Default:	Yes
Selection:	Yes or No
Yes	Enable RPS sessions over the SDI bus.
No	Do not enable RPS sessions over the SDI bus.

Enable SDI RPS determines if the control panel allows RPS communications over the SDI bus. This item must be set to **Yes** if you plan to use the external modem configuration, a private LAN or WAN, or local RPS programming.



If the reset pin is in the locked position, local RPS programming is allowed even if this prompt is set to **No**.



When **Enable SDI RPS** is configured to allow for local programming, Jumper 8 in the SIM must be shorted or closed, power must be removed and reapplied after changing the address, and a standard serial null-modem cable is required.

Call Back Enabled

Default:	No
Selection:	Yes or No
Yes	When the control panel hears the correct RPS password (refer to RPS Passcode in <i>Section 2.7 RPS Parameters</i> on page 32), it ends the SDI RPS session and then reconnects to RPS using the RPS IP Address if Enable Ext Modem is set to No . If Enable Ext Modem is set to Yes , the control panel re-establishes communication with RPS using the RPS Dial String. This ensures that the control panel communicates only with valid RPS units.
No	The SDI RPS session starts immediately; no call-back is required. The control panel can engage in SDI RPS sessions regardless of the originating location.

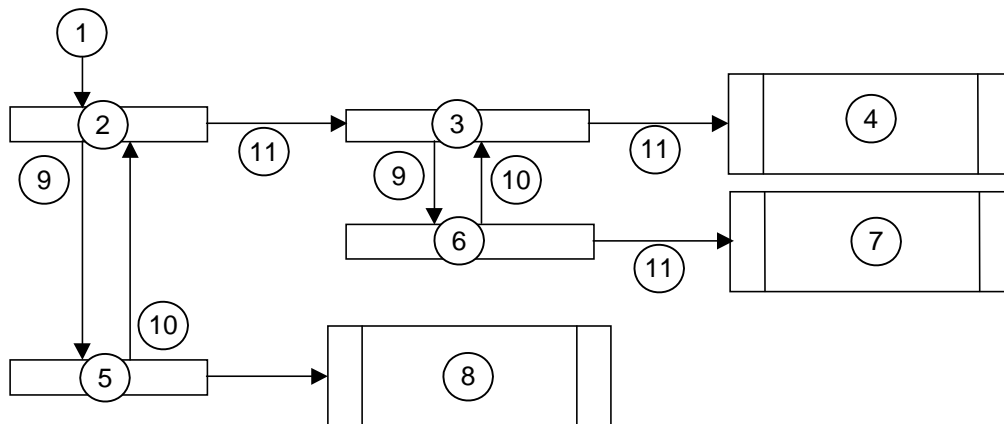
Using this function allows the control panel, after verifying the RPS passcode, to provide an additional level of security. Before allowing any upload or download, it ends the SDI RPS session and then reconnects with RPS using one of the following:

- The RPS IP Address (**Enable Ext Modem** must be set to **No**)
- The RPS Dial String (**Enable Ext Modem** must be set to **Yes**)



Do not enable RPS Call Back when using an external modem.

Figure 6: COMMAND 43 Flow Chart



1 - COMMAND 43

2 - **Contact RPS?**3 - **RPS via Phone?**

4 - Seizes phone line and calls RPS

5 - **Answer now?**6 - **RPS by network?**7 - *Begins RPS session over the network*8 - *Seizes phone line and begins RPS session*

9 - [PREV]

10 - [NEXT]

11 - [ENT]

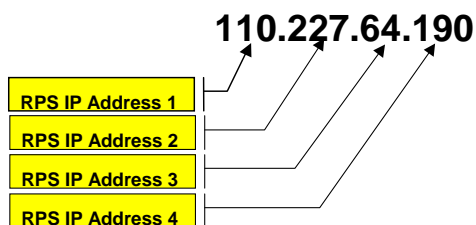
RPS IP Address 1**Default:** 0**Selection:** 0 to 255

0 to 255

Enter the first three digits of the IP address. Leading zeros are not required.

This prompt and the next three prompts determine the IP address for RPS.

An IP address has four fields. Each field has a range of 0 to 255. For example, an IP address is expressed as 110.227.64.190. (Refer to *figure 7*.) The D5200 programmer divides the IP Address into four programmable fields. Contact your network administrator to determine the IP address to which the RPS computer is connected.

figure 7: RPS IP Address Prompts

Set **RPS IP Address** to 0 if **Enable Ext Modem** is set to **Yes**.

RPS IP Address 2**Default:** 0**Selection:** 0 to 255

Refer to **RPS IP Address 1**.

RPS IP Address 3**Default:** 0**Selection:** 0 to 255

Refer to **RPS IP Address 1**.

RPS IP Address 4**Default:** 0**Selection:** 0 to 255

Refer to **RPS IP Address 1**.

RPS Port Number**Default:** 7700**Selection:** 1 to 65535

This prompt specifies the destination port for outgoing RPS session requests to the IP address specified in **RPS IP Address #**.

6.4.2 Using an External Modem

Through the use of a standard, off-the-shelf modem (capable of communicating at 9600 baud) and a D9133DC connected directly to the control panel, RPS can communicate with a D9412GV3 or D7412GV3 at speeds of up to 9600 baud.



Both the U.S. Robotics V.92 56 K Modem (model No. 5686, includes V.92 and V.90 56 K standard technology) and the Best Data Smart One V.92/V.44 56 K External Data/Fax Modem (model # 56SX-92) are recommended for use as external modems (connected to the control panel) based on compatibility testing by Bosch Security Systems, Inc. Other modules were not tested or were incompatible.

The seven prompts on page 133 help to configure the requirements necessary to connect an external modem to a D9412GV3 or D7412GV3 Control Panel using a D9133DC. This configuration allows communication with RPS at 9600 baud because data is routed through the SDI bus.



Use a separate phone line if an external modem is being connected to the control panel by a D9133DC Direct Connect Programming Module. If obtaining a different phone line from the line used by the control panel is impossible, ensure that the control panel is wired in front of any premises phone and the external modem devices so that full line seizure is maintained. Also, ensure that the following items are programmed in *Section 2.7 RPS Parameters* on page 32:

- **Answer Armed** = 1 to 15
- **Answer Disarmed** = 1 to 15
- **RPS Line Monitor** = No
- **RPS Call Back** = No
- **RPS Phone number** = Blank



When using an external modem, initialize it using the following HyperTerminal procedure on your computer. The HyperTerminal procedures can vary, depending upon the operating system.

1. In Windows, open the HyperTerminal application. Select:
Programs→Accessories→Communications
2. Connect the modem to an available COM port.
3. With the modem connected, select the appropriate COM port within HyperTerminal. Refer to *Figure 8*.
4. Set the baud rate of the modem to 9600.



For Best Data Smart One V.92:

Type [A][T][S][3][7][=][9][Enter]

For US Robotics:

Type [A][T][&][N][6][Enter]

For other modems, consult the instructions provided with the device for the correct text string.

5. Type [A][T][E][0][Enter]. This eliminates echo, making all user input from this point forward invisible on the screen.
6. Type [A][T][&][W][0][Enter] to write the configuration to modem memory. The modem profile is saved to a file upon disconnection or power loss.

The external modem is connected to the D9133DC Direct Connect Programming Module that is connected to the SDI bus using SDI Address 88. Refer to *Figure 9* on page 131. A standard serial cable is required to connect the D9133DC to the external modem.



If you are using an external modem for RPS communications, the enhanced communications and RPS functions using a NIM are disabled.

Figure 8: Com Port Selection within HyperTerminal

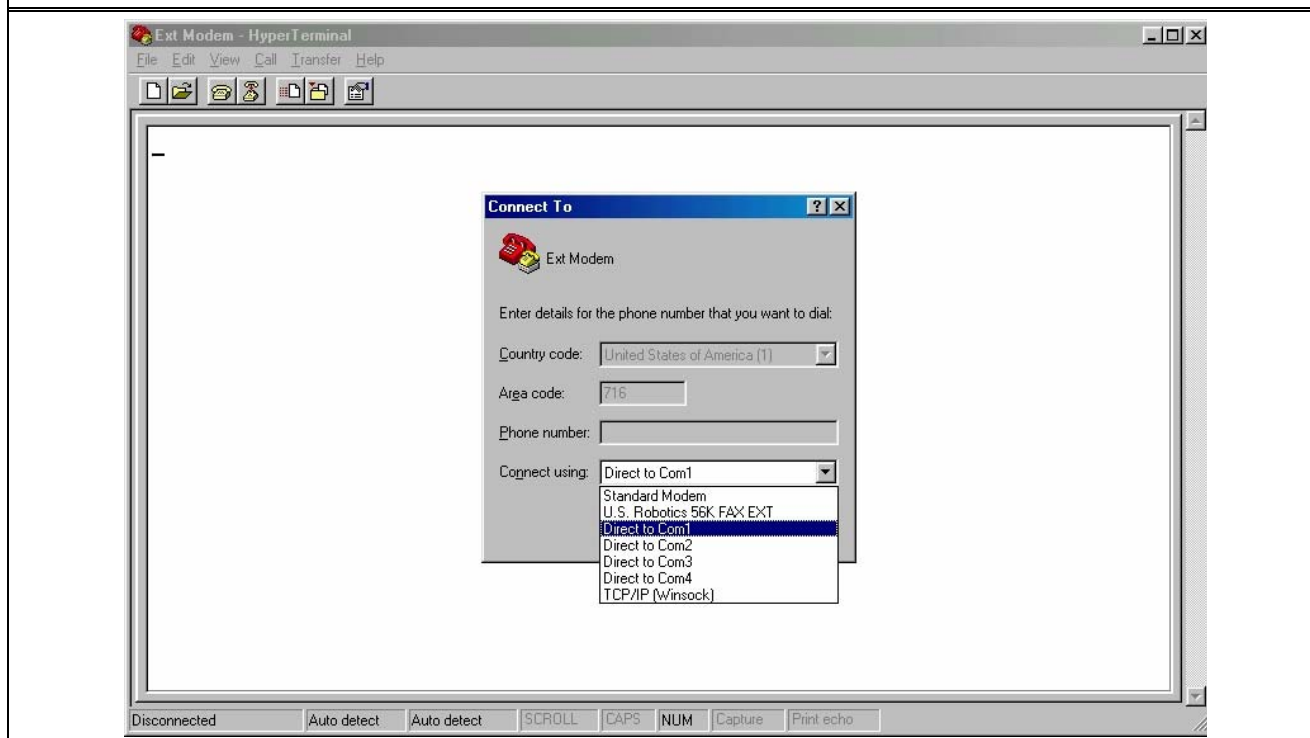
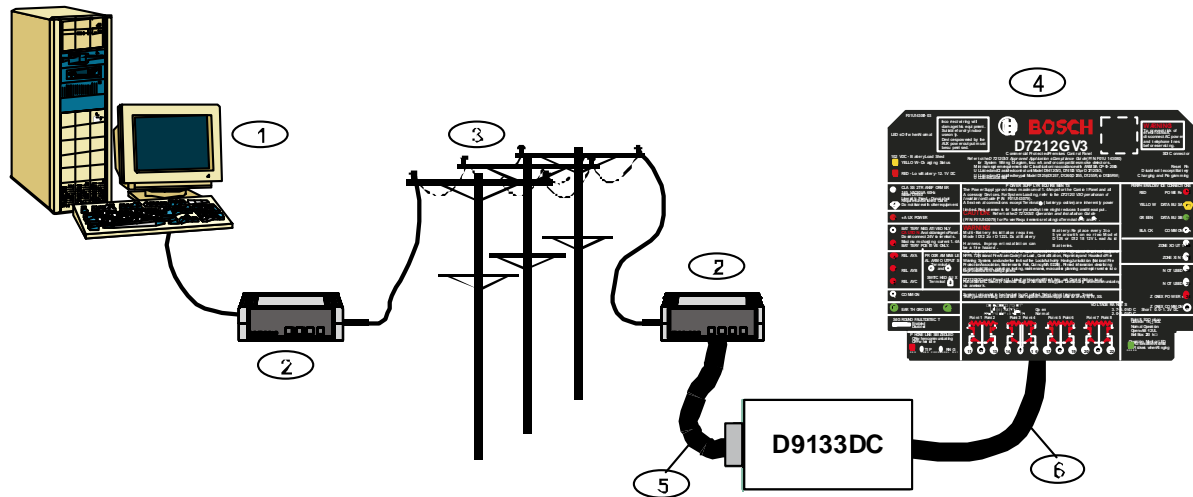


Figure 9: External Modem Connection

- 1 - PC running Remote Programming Software (RPS)
- 2 - Modem
- 3 - PSTN

- 4 - D9412GV3/D7412GV3 Control Panel
- 5 - Standard null modem cable
- 6 - SDI bus



To use an off-the-shelf external modem and a D9133DC serial module to connect to the control panel using RPS, use the following settings:

1. GV2AUX\ENHANCED COMM\Enhanced Comm\No
2. GV2AUX\SDI RPS PARAMETERS\Enable SDI RPS\Yes
3. GV2AUX\SDI RPS PARAMETERS\Callback Enabled\No
4. GV2AUX\SDI RPS PARAMETERS\RPS IP Address 1-4\0
5. GV2AUX\SDI RPS PARAMETERS\Enable Ext Modem\Yes
6. GV2AUX\SDI RPS PARAMETERS\Answer Armed\1 to 15
7. GV2AUX\SDI RPS PARAMETERS\Answer Disarmed\1 to 15
8. GV2AUX\SDI RPS PARAMETERS\RPS Line Monitor\No
9. GV2AUX\SDI RPS PARAMETERS\Seize Relay\No
10. GV2AUX\SDI RPS PARAMETERS\Modem Init String\ATE0
11. GV2AUX\SDI RPS PARAMETERS\RPS Dial String\ (blank)
12. GV2AUX\SDIRPS/ENHANCED CONF\Baud Rate\9600
13. GV2AUX\SDIRPS/ENHANCED CONF\Parity/Stop No\1
14. GV2AUX\SDIRPS/ENHANCED CONF\RTS Control\ON
15. GV2AUX\SDIRPS/ENHANCED CONF\DTR Control\ON
16. GV2AUX\SDIRPS/ENHANCED CONF\9133 Supervision\No
17. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG1 Primary SDI\No
18. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG1 Backup SDI\No
19. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG2 Primary SDI\No
20. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG2 Backup SDI\No
21. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG3 Primary SDI\No
22. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG3 Backup SDI\No
23. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG4 Primary SDI\No
24. GV2MAIN\PANEL WIDE PARAMETER\Enhanced Routing\RG4 Backup SDI\No
25. The control panel reset pin can be up or down.
26. The modem at the control panel location must be set for 9600 baud and echo off. This information must be written to the modem configuration area. Hyperterminal can be used to send the following Hayes modem commands (refer to the modem's manual for command syntax):
 - ATS37=9 (set baud rate to 9600)
 - ATE0 (eliminate echo)
 - AT&W0 (write configuration to modem memory, not echoed)
27. Ensure that the modem at RPS is set up for 9600 baud.
28. From the control panel communication window on RPS, connect by modem at 9600 baud.

Enable Ext Modem

Default: No	
Selection: Yes or No	
Yes	Enable SDI Address 88 for use with an external modem.
No	Disable SDI Address 88 for use with an external modem.

Setting this item to **Yes** instructs the control panel that SDI Address 88 is enabled for use with an external modem. For further information on Local RPS programming, refer to the *RPS Installation and Operation Guide* (P/N: 4998141259).

<input checked="" type="checkbox"/>	Setting this item to Yes disables Enhanced Communication and SDI RPS for use over a LAN or WAN.
-------------------------------------	--

Answer Armed

Default: 7	
Selection: 0 to 15	
0	No answer when all areas are Master Armed.
0 to 15	The control panel answers the phone after the specified number of rings when all areas are Master Armed.

Determines the number of rings after which the external modem automatically answers a call if all areas are Master Armed.

Answer Disarmed

Default: 7	
Selection: 0 to 15	
0	No answer when any area is Perimeter Armed or Disarmed.
0 to 15	The control panel answers the phone after the specified number of rings when any area is Perimeter Armed or Disarmed.

Determines the number of rings after which the external modem automatically answers a call if any area is Perimeter Armed or Disarmed.

RPS Line Monitor

Default: No
Selection: Yes or No

Not used. Keep this item set to **No**.

Seize Relay

Default: No
Selection: Yes or No

Not used. Keep this item set to **No**.

Modem Init String

Default: ATE0
Selection: A to Z (capital letters only), 0 to 9, [SPACE], ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _

Determines which initialization string the control panel sends to the external modem when the control panel powers up.

<input checked="" type="checkbox"/>	If special characters are required, Modem Init String can be programmed successfully only from RPS. The D5200 Programmer allows only the characters shown in the Modem Init String default selections.
-------------------------------------	--

RPS Dial String

Default: ATDT
Selection: Not available

Not used.

6.5 Programming Path Numbers and IP Addresses for Enhanced Communications

Enhanced communications is the ability to communicate by some means other than the standard digital dialer. In this section, programmable parameters allow you to define up to four separate enhanced communication paths to which events can be routed. To route an event (such as an Alarm or Trouble) to an enhanced communication path, additional programming must also be completed in *Section 2.3 Routing* on page 16 and *Section 2.4 Enhanced Routing* on page 24.

Enhanced Comm

Default:	No
Selection:	Yes or No
Yes	Enable enhanced communications over the SDI bus.
No	Do not enable enhanced communications over the SDI bus.



If using IP Addresses as the communication means for UL 864 Commercial Fire applications, set this parameter to **Yes**.

Determines if the control panel allows enhanced communications over the SDI bus.



- **Modem Format** must be set to **Yes** when using enhanced communications.
- **Enable Ext Modem** must be set to **No** if enhanced communications are used.
- **Enhanced Comm** must be set to **No** if an external modem is used.



To disable Enhanced Routing completely over an SDI path, **RG#Primary SDI**, **RG#Backup SDI**, and **Enhanced Comm** prompts must all be set to **No**.

Events can be routed to as many as four available enhanced communication paths through the SDI bus. If an event (or group of events) is routed to an SDI path, the number entered in Primary Device determines which SDI path is used (provided that **RG# Prim, Primary SDI** was set to **Yes** in Routing).

If events are to be routed to an IP address (in a private LAN or WAN application), determine which path is used (Path 1 to Path 4), and enter the appropriate IP Address for that path (refer to **Path # IP Add1** to **Path # IP Add4**).

If events are to be routed to an SDI Path but not to an IP Address, allow the setting for **Path # IP Add#** to remain at 0. **Path # Poll Rate**, **Path # Ack Wait**, and **Path # Retry Count** must be programmed.

Path # IP Add1

Default:	0
Selection:	0 to 255
0 to 255	Enter the first three digits of the IP address. Leading zeros are not required.

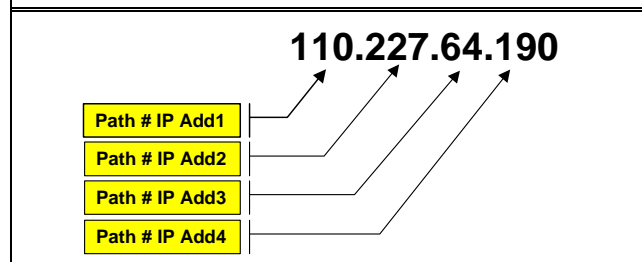


If using IP Addresses as the communication means for UL 864 Commercial Fire applications, set **Path # IP Add 1** through **4** as necessary.

Path # IP Add 1 and the next three items determine the IP addresses for each of the four enhanced communication paths available when using the D5200.

An IP address has four fields. Each field has a range of 0 to 255. For example, an IP address is expressed as 110.227.64.190. The D5200 programmer splits the IP address into four programmable fields (refer to *Figure 10*). Contact your network administrator to obtain the appropriate IP Address to contact a central station receiver.

Figure 10: Path # IP Add1 to Add4



Path # IP Add2

Default:	0
Selection:	0 to 255

Refer to **Path 1 IP Add1**.

Path # IP Add3

Default:	0
Selection:	0 to 255

Refer to **Path 1 IP Add1**.

Path # IP Add4**Default:** 0**Selection:** 0 to 255Refer to **Path 1 IP Add1**.**Path # PortNum****Default:** 7700**Selection:** 1 to 65535

This prompt specifies the destination port number for each of the four enhanced communication route path destinations.



Whenever an IP address or port number configured in the control panel is changed, the central station must resynchronize the control panel's anti-replay/anti-substitution static key.

Path # Poll Rate**Default:** 0**Selection:** 0, 5 to 65535 sec

0	Disables the heartbeat poll (not recommended, refer to the first Important Note that follows).
5 to 65534	Enables the poll rate for the amount of time programmed here.
65535	The maximum number of 65535 sets the poll rate to once every 24 hr.

This prompt and the next two prompts determine how the SDI Path is supervised between the SDI device and the central station receiver(s). Do not confuse the SDI Path supervision with the supervision of the SDI device itself (the connection of the SDI device to the control panel). Each SDI Path can be configured to transmit a Heartbeat Poll to the central station for supervision purposes. This ensures the integrity of the connection at all times.



If using IP Addresses as the communication means for UL 864 Commercial Fire applications, program this parameter as necessary.



In order to supervise the virtual link between the control panel and a central

station receiver over a network path, you **must** set **Path # Poll Rate** to a non-zero value.



If the control panel is programmed to send Heartbeat Poll to the central station, a rate of 75 sec maintains the virtual link in most network configurations. Decreasing the value for **Path # Poll Rate** increases the amount of idle communication between the SDI device and the central station receiver. Increased idle communication between the control panel and the receiver decreases the control panel's event reporting efficiency.



The control panel readjusts the Heartbeat Poll rate temporarily to less than 300 sec to 300 sec when online with RPS. The poll rate returns to the programmed value after the RPS session ends.

The value programmed in **Path # Poll Rate** is the interval at which the control panel sends a Heartbeat Poll to the central station receiver. The value programmed in **Path # Ack Wait** is the length of time the control panel waits for an acknowledgment of a Heartbeat poll. If the acknowledgment is not received, the control panel checks to determine if the **Path # Retry Count** entry is greater than 0. If so, the control panel retries the number of times programmed (in **Path # Retry Count**) to send the Heartbeat Poll before declaring the Path failed and generating a COMM TROUBLE SDI ## for SDI 88

(Path 1 = SDI 88, Path 2 = SDI 89, Path 3 = SDI 90, Path 4 = SDI 91) Event. For SDI 92 (Path 1 = SDI 92, Path 2 = SDI 93, Path 3 = SDI 94, Path 4 = SDI 95) event.

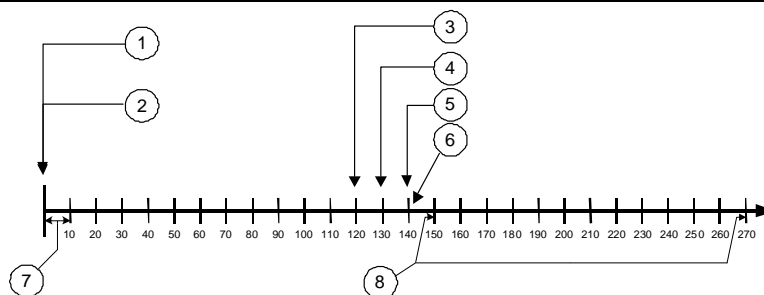
If **Path # Poll Rate** is programmed with a value and the central station does not acknowledge the poll from the control panel, keypads annunciate a trouble condition. To send this event to the central station, refer to the **Comm Trouble** prompt in *Section 2.13.2 Panel-Wide Relays* on page 81.

Example of Heartbeat:

- **Path # Poll Rate** is set to 120 sec
- **Path # Ack Wait** time is set to 10 sec
- **Path # Retry Count** is set to 2

When the control panel first powers up, the first Heartbeat Poll for Path 1 is sent and is acknowledged in 1 sec. 120 sec after the first Heartbeat Poll is sent, the second Heartbeat Poll for Path 1 is generated and sent to the central station receiver.

Figure 11: Poll Rate Timeline



- | | |
|--|---|
| 1 - Heartbeat Poll sent | 5 - No acknowledgment, Heartbeat re-sent, retry #2 |
| 2 - Acknowledgment received | 6 - Path declared failed |
| 3 - Second Heartbeat Poll sent | 7 - 10-sec interval |
| 4 - No acknowledgment, Heartbeat re-sent, retry #1 | 8 - Additional Heartbeats sent at the poll rate time until acknowledged |

Example of Retry Count:

An acknowledgment of the heartbeat was not received within 10 sec. The control panel sends the next Heartbeat Poll after the first 10-sec ACK wait period expires. If the central station does not acknowledge this Heartbeat Poll, the control panel continues to re-send. When the resend count is reached, the control panel declares this path as failed (and generates the Comm Trouble ## Event). The control panel continues to re-send the Heartbeat Poll at the original poll rate time until it receives an acknowledgment, even after declaring a Comm Trouble.

When the control panel receives acknowledgment from the central station, the control panel returns to the normal Poll Rate (which, in this example, is 120 sec).

If more than one SDI Path is used, the control panel handles them on a successive basis. For example, if acknowledgment from SDI Path 1 is not received within 10 sec (using the previous example), the control panel moves to SDI Path 2 to send its Heartbeat Poll (and subsequently waits for the ack) before returning to SDI Path 1 to re-send its heartbeat.



If Heartbeat Polls are enabled to send by an SDI path, and the **Path # Ack Wait** time is exceeded, a COMM TRBL SDI ## event occurs. When this condition occurs, all events routed to this path go immediately to the backup path destination.

Entries are made in one-sec increments.



Although RPS and the D5200 allow **Path # Poll Rate** values of 1 to 4, the control panel interprets these entries as an entry of 5.



5 min = 300 sec
1 hour = 3600 sec
12 hours = 43,200 sec
18 hours = 64,800 sec

Path # Ack Wait

Default: 13

Selection: 0, 5 sec to 65535 sec

0	The control panel does not look for any acknowledgment from the central station.
5 to 65535	The control panel waits this amount of time to receive an acknowledgment from the central station.

Determines how long the control panel waits for an acknowledgment from the central station after a Heartbeat Poll or an actual event was transmitted. This prompt is applicable to SDI transmitted events and Heartbeat Polls. Entries are made in one-sec increments.



If using IP Addresses as the communication means for UL 864 Commercial Fire applications, this parameter cannot be zero (0).



Although the D5200 allows **Path # Ack Wait** values of 0 to 4, the control panel interprets these entries as an entry of 5 sec.

Path # Retry Count

Default: 5

Selection: 0 to 255

0	COMM FAIL RG# SDI ### Events are not generated.
1 to 255	COMM FAIL RG# SDI ### Events are generated after resending Heartbeat Poll the number of times selected for a given SDI path.

Determines how many times the control panel resends the Heartbeat Poll before declaring a path failure and generating a COMM FAIL RG# SDI ### (RG # = 1 to 4, SDI ### = 88 for Path 1, 89 for Path 2, 90 for Path 3, 91 for Path 4) Event.



If using IP Addresses as the communication means for UL 864 Commercial Fire applications, program this parameter as necessary.

The default settings meet or exceed the UL specifications.

Path # Anti-Replay**Default:** No**Selection:** Yes or No*

* Anti-replay is always enabled on the control panel. The D5200 Handheld Programmer selection of No does not disable anti-replay.

Anti-replay is a strategy that counters “replay” attacks. This feature prevents a malicious attack that substitutes a control panel or another network interface module (NIM) from delivering counterfeit events over a network in place of events sent by the actual control panel. A replay attack occurs when someone records a message sent over the network by Device A, and replays this message at a later time while pretending to be Device A.

Anti-replay is always enabled on D9412GV3 and D7412GV3 control panels.



You must also enable the **Substitution Monitor** function in the Conettix D6600 Communications Receiver/Gateway. Refer to *Substitution Monitor* in the *Conettix D6600/D6100 Receiver Gateway Program Entry Guide* (P/N: 4998122702) for more details.

Account Identification

The D6600 Receiver can identify the network accounts by either the IP address or the account number received in the message sent from the control panel. The account number sent in the message is always the account number for Area 1. Although you can program up to ten digits for the account number, only eight digits are sent in the message to the D6600 Receiver.

6.6 SDI RPS/Enhanced Communications Configuration

This section provides the necessary prompts for configuring the SDI-Network Interface Module (NIM) when using it for SDI RPS or SDI enhanced communication applications.

Baud Rate**Default:** 9600**Selection:** 300, 1200, 2400, 4800, 9600, 14.4 K

This item determines the communication baud rate for the network interface module (NIM). Because the SDI bus communicates at 9600 baud, keep this prompt at 9600 baud. Pressing the [SPACE] bar on the D5200 toggles through the available options.



Do not set this value to any setting other than 9600 baud.

Parity/Stop**Default:** No/1**Selection:** No/1, No/2, Odd/1, Even/1

No/1 No parity, 1 stop bit.

No/2 No parity, 2 stop bits.

Odd/1 Odd parity, 1 stop bit.

Even/1 Even parity, 1 stop bit.

This prompt addresses two items: parity and the number of stop bits for the network interface module (NIM). Pressing the [SPACE] bar on the D5200 toggles through the available options.



Set this item to No/1 when using the External Modem feature.

RTS Control**Default:** On**Selection:** On, AutoX, Off, AutoR

On Sets RTS to on (hardware control).

Auto X Automatically enables Xon/Xoff (software control).

Off Sets RTS off (hardware control).

Auto R Sets this to Auto RTS.

Determines how the Request To Send (RTS) control parameters are defined for the network interface module (NIM). Pressing the [SPACE] bar on the D5200 toggles through the available options.



Set this item to On when using the External Modem feature.

DTR Control**Default:** On**Selection:** On, AutoD, Off

On Sets DTR to on (hardware control).

AutoD Sets this to Auto DTR.

Off Sets DTR off (hardware control).

Determines how the Data Terminal Ready (DTR) control parameters are defined for the network interface module (NIM). Pressing the [SPACE] bar on the D5200 toggles through the available options.



Set this item to On when using the External Modem feature.

Supervise SDI 88

Default:	No
Selection:	Yes or No
Yes	Supervise the network interface module (NIM) at SDI address 88.
No	Do not supervise the network interface module (NIM) at SDI address 88.

This item determines whether the NIM is supervised. If the NIM is supervised, disconnecting it from the control panel creates a Trouble SDI 88 Event and the keypad annunciates a trouble tone and displays **SERV SDI 88**.

Supervise SDI 92

Default:	No
Selection:	Yes or No
Yes	Supervise the network interface module (NIM) at SDI address 92.
No	Do not supervise the network interface module (NIM) at SDI address 92.

This item determines whether the NIM is supervised. If the NIM is supervised, disconnecting it from the control panel creates a Trouble SDI 92 Event and the keypad annunciates a trouble tone and displays **SERV SDI 92**.



Trouble SDI 88 or SDI 92 Reports are always reported using the account number for Area 1.

6.7 Route Group Rates

These parameters enable a Route Group to switch to the faster **Path # Poll Rate** when the following conditions apply:

- Both primary and backup devices use enhanced communication via an SDI device.
- Both primary and backup path destinations are the same (this includes IP address and port).

- Both primary and backup paths use different poll rates.
- Either the primary or the backup path (not both) has a Communication Trouble condition.

RG# 1 Faster Rate

Default:	No
Selection:	Yes or No
Yes	Upon detection of a Communication Trouble on either the primary or backup enhanced communication paths, the working path immediately changes to the faster poll rate.
No	Upon detection of a Communication Trouble on either the primary or backup enhanced communication paths, the working path continues to use the configured poll rate.

6.8 Miscellaneous

Fire Summary Sustain

Default:	No
Selection:	Yes or No
Yes	Forces the Summary Fire relay output to remain on after the Alarm Silence command.
No	Allows Summary Fire relay output to be silent when the Fire Alarm Bell output is silenced and all Fire Points return to normal.

Use this parameter to set the Summary Fire relay output to continue or to stop after the Fire Alarm Bell is silenced or times out. Refer to the **Summary Fire** prompt in *Section 2.13.2 Panel-Wide Relays* on page 82.

Fire Supv Res Type

Default:	0
Selection:	0, 1, 2
0	The control panel sends a FIRE TROUBLE RESTORE when a Fire Supervision point restores to normal.
1	The control panel sends a FIRE ALARM RESTORE when a Fire Supervision point restores to normal.
2	The control panel sends a FIRE SUPERVISION RESTORE when a Fire Supervision point restores to normal.

Determines how the control panel sends a Fire Supervision Restoral Event.



The Fire Supv Restore Event is part of Fire Events in Routing. If Fire Supervision Restore Events are needed, simply enable them in Routing.

Enable Protocol Type

Default:	No
Selection:	Yes or No

Not required. Leave at default value.

Fire Trouble Resound

Default:	0
Selection:	0, 1, 2
0	Keypads do not re-sound the fire trouble tone.
1	Keypads re-sound the fire trouble tone at 12:00 PM if any Fire point that falls within the scope of a keypad is in an off-normal condition.
2	Keypads re-sound the fire trouble tone at 12:00 AM if any Fire point that falls within the scope of a keypad is in an off-normal condition.

This item determines if a fire trouble condition, previously acknowledged and silenced at a keypad, automatically (locally) re-sounds the fire trouble tone at 12:00 PM, 12:00 AM, or not at all if the point is still in an off-normal state. Events are not generated at the time the re-sound occurs.

Early Ambush Timer

Default:	10 min
Selection:	5 to 30 min

The programmed time is the maximum value of the Early Ambush Timer. When Early Ambush is set to **Yes** for a specified area (refer to *A# Early Ambush* on page 48) and the area is disarmed, the user has the amount of time programmed here to enter a second code into the keypad.

If a second passcode is not entered within the programmed time, a Duress event is generated based on the first user code. Duress reports must be enabled in Routing in order to be sent to a central station.

Secondary Ambush Code

Default:	Unique
Selection:	Unique or any
Unique	The code used to end the timer must be different from the code used to disarm the area.
Any	The timer can be stopped using a different code, or the same code that disarmed the area.

The Secondary Ambush Code determines whether the same passcode can be used to begin and end the Early Ambush process.

Abort Window

Default: 30 sec
Selection: 15 to 45 sec

This parameter determines the amount of time the control panel delays a Burglar Alarm event from a point with **P## Alarm Abort** set to **Yes**. If an alarm silence operation is performed before this time elapses, the alarm transmission is aborted and the keypad shows an optional ALARM NOT SENT message. When an alarm transmission is successfully aborted, no event is written to the control panel event log.

When an abort alarm timer starts, it does not stop until an alarm silence operation is performed or the time expires.



This feature does not apply to Fire Alarms or invisible point alarms.

For SIA CP-01 Compliance:

Abort Window is a required parameter.



To meet UL requirements, the combined Entry Delay time and Abort Window time must not exceed 60 sec. For Entry Delay time programming information, refer to **P## Entry Delay** in the *Point Responses* section of your control panel's program entry guide.

UL note: Maximum settings for residential use:

Exit Delay – 120 sec
 Entry Delay = 45 sec bell
 Off-Premise Transmission = 60 sec

Maximum settings for commercial use:

Exit Delay – 120 sec no line security
 Entry Delay = 60 sec bell
 Off-Premise Transmission = 60 sec

The system must use both the bell and off-premise transmission.

Passcode Length

Default: 0
Selection: 0, 3, 4, 5, or 6

0	Sets a variable length for user passcodes, allowing for backward compatibility
3, 4, 5, or 6	Sets a fixed length to all user passcodes.

During entry delay, the code is accepted when the last digit is pressed to disarm the area.

For SIA CP-01 Compliance:

Passcode Length must be set to 3, 4, 5, or 6.

Swinger Count

Default: 1
Selection: 1, 2, 3, or 4

1, 2	Number of fault or trouble bypasses allowed per hour for SIA CP-01 compliance.
3	Optional fault count
4	Value used for backward compatibility with previous control panel operation.

When a point has **P# Swinger Byps** set to **Yes**, the value set in **Swinger Count** determines the number of times the point is faulted erroneously within an hour before it is automatically bypassed.

For SIA CP-01 Compliance:

P## Swinger Byps can be **Yes** or **No**.

If **P## Swinger Byps** is **Yes**, **Swinger Count** must be 1 or 2.

Remote Warning

Default:	Yes
Selection:	Yes or No
Yes	The system uses the Alarm Bell output to annunciate the arming and disarming of an area through remote software, or a remote arming device such as a key switch or key fob.
No	No remote warning occurs to annunciate the arming and disarming of an area through remote software, or a remote arming device such as a key switch or key fob.

Upon remote arming, the output pulses on for 2 sec.
Upon remote disarming, the output pulses on, off, on, off for 2 sec each.

For SIA CP-01 Compliance

Remote Warning must be set to **Yes**.

CrystalTime Adj

Default:	No
Selection:	Yes or No
Yes	Set the clock time control on the control panel to the on-board crystal frequency.
No	Do not set the clock time control on the control panel to the on-board crystal frequency.

When set to **Yes**, the control panel switches its clock time control from the traditional AC frequency to the on-board crystal frequency.

Perimeter Relay

Default:	No
Selection:	Yes or No
Yes	Change the function of the area-wide fail-to-close relays to follow the perimeter armed states of their areas.
No	The area-wide fail-to-close relay operates normally.

When set to **Yes**, the **A# Fail to Close** relay becomes an area-wide perimeter armed relay. This relay is activated when all areas assigned to the same relay have perimeter points that are armed.

Early Armed Relay

Default:	No
Selection:	Yes or No
Yes	Change activation of Area Armed or Perimeter Armed Relay to the beginning of the exit delay time.
No	Maintain the activation of Area Armed or Perimeter Armed Relay at the end of the exit delay time.

When this prompt is set to **Yes**, the Area Armed or Perimeter Armed Relay activates at the beginning of the exit delay time.

6.9 Cross Point Parameters

This section discusses the requirements necessary to program Cross Point functions.



Use the Cross Point function on non-fire points only.

The Cross Point option reduces false alarms. Points can be programmed so that the control panel needs to see an Alarm condition within a programmed period of time (called Cross Point Time) from at least two points within a Cross Point Group (*Table 43*) before Cross Point Alarm Events are generated. These points must have **P## Cross Point** set to **Yes** to generate this event.

There are 31 Cross Point Groups in the D9412GV3 and ten in the D7412GV3. Each Cross Point Group consists of eight points and is identified by the point numbers in them (for example, Cross Points 1 to 8, Cross Points 9 to 16, and so on). The maximum number of points that can be programmed to meet the Cross Point criteria is two. Point numbers from different Cross Point Groups do not affect each other. Refer to *Table 43* for a complete listing of Cross Points comprising each Cross Point Group.

When any point with **P## Cross Point** set to **Yes** detects an alarm condition, the control panel starts a timer as programmed in the **Cross Point Time** prompt.

If a second Cross Point within the same Cross Point Group detects an alarm condition, the control panel creates a Cross Point Alarm Event for both points, provided both points activate inside the Cross Point Window. A Cross Point is considered to be in alarm when it meets the criteria for Instant Alarm response. The Cross Point index must have **P## Pt Response** set to a value that generates an instant alarm response.

If a single Cross Point detects an alarm and stays faulted throughout the duration of the Cross Point Window, a standard Alarm Report is generated for that point.

Conversely, if a single Cross Point detects an alarm, then restores, and no other conditions occur, an Unverified Event is generated for that point. A second alarm on the first point does not create an Alarm Event but rather an Unverified Event.

Table 43: Cross Point Ranges Within Groups

Cross Point Group	Point Range		
1	1	to	8
2	9	to	16
3	17	to	24
4	25	to	32
5	33	to	40
6	41	to	48
7	49	to	56
8	57	to	64
9	65	to	72
10	73	to	80
11	81	to	88
12	89	to	96
13	97	to	104
14	105	to	112
15	113	to	120
16	121	to	127
17	129	to	136
18	137	to	144
19	145	to	152
20	153	to	160
21	161	to	168
22	169	to	176
23	177	to	184
24	185	to	192
25	193	to	200
26	201	to	208
27	209	to	216
28	217	to	224
29	225	to	232
30	233	to	240
31	241	to	247

Refer to *Section 2.3 Routing* on page 16 for information about programming the destination (for example, the central station) for Unverified Events. An Unverified Event does not produce a corresponding Restoral Event.

The Cross Point function applies only to alarm conditions. It does not apply to supervisory or trouble conditions. Points programmed with point response D (Delayed) eventually enter into an alarm condition if the area is not disarmed in time.

Cross Point Time

Default: 20 sec
Selection: 5 sec to 255 sec

Select the amount of time (in seconds) that points within a Cross Point Group are in alarm before a Cross Point event is generated.

7.0 RADXAXS

7.1 Door Profile

This programming category is used to:

- Assign an area that also activates the D9210B
- Assign a point to the door
- Program the door state to change the time when the arm state changes
- Allow for the Strike relay to activate upon a fire alarm
- Programming the Interlock point.

Door

Default: 1
Selection: 1 to 8

Enter the number of the door you are programming.



The D9412GV3 supports up to eight doors. The D7412GV3 supports two doors.

D# Entry Area

Default: Blank	
Selection: Blank, 1 to 8	
1 to 8	The area assigned to the door controller to which the reader allows access.
Blank	Door controller does not function.

Assign an area to the door controller. This entry allows the D9210B to be polled, activating communication to the control panel. This is also the area a user exits when initiating an REX.



All SDI devices, regardless of area assigned, report to Area 1, Account 1 by default upon SDI failure. If a D9210B becomes disconnected, an SDI Fail ## and a Missing Point ### Event is created.



If the D9210B is not programmed with a **D# Entry Area**, 9210 NOT READY

appears at the keypad with this door assigned to it when you press the [ENTER] key

D#CC#Scope

Default: Blank	
Selection: Blank, 1 to 8	
1 to 8	Determines disarming rights. The user's access level and the CC # Scope determines which areas are disarmed.
Blank	Only the area assigned to the D# Entry Area disarms this door.

Enter the keypad number (CC#) which determines the scope of the user ID's disarming rights. Areas disarm on the basis of this keypad's scope and the authority level of the user.

D# Custom Function

Default: 0 (Disabled)	
Selection: 0, 128-143	
0	Custom function disabled.
128-143	The custom function number that executes upon a valid ID, given the appropriate user access level and area arm state.

You can program a custom function to run at the keypad programmed for **CC# Scope**. This custom function activates only for users with an **L## Function Level?** Assignment (refer to *Section 2.11 User Interface* on page 76) in which a valid ID can execute a custom function during the armed or disarmed state. The user number to which the token is assigned must have an assigned passcode.

If **D# Disarm On Open** is set to **Yes** for the same door, and **L## Function Level?** is set to D or C, the custom function executes when the door is physically opened.



A user's access level and the armed state of the area determine whether the custom function activates. This access level is programmed in the **L## Function Level?** prompt. Refer to *2.11 User Interface* on page 60.

Table 44 on page 145 shows how this programming affects custom function activation.

Table 44: Effects of Programming on Custom Function Activation

L## Function Level?	Custom Function Activation
M (Armed)	User token activates the custom function assigned to the Door Controller only while the entry area for the Door Controller is Master Armed or Perimeter Armed.
D (Disarmed)	User token activates the custom function assigned to the Door Controller only while the entry area for the Door Controller is disarmed.
C (Armed and Disarmed)	User token activates the custom function assigned to the Door Controller regardless of the armed state of the entry area.
Blank	User token does not run the custom function assigned to the Door Controller.



A user's security level must have an M, P, or D to operate the custom function.

D# Door Point

Default:	Blank
Selection:	Blank, 1 to 127, 129 to 247
1 to 127, 129 to 247	The point number assigned to this door. Points 128 and 248 are reserved by the control panel for internal use.
Blank	No point number is assigned to this door.

Enter the point number assigned to this door. This point cannot be used for any other point assignments.



Door points must be programmed as Perimeter points. If a 24-hour point type is required for the Door point, you can use a Perimeter point type with a point response of 9 to C. Also, the debounce count must be set to 4 in Point Assignments.



When assigning Points 1 to 8 (control panel zones), the end-of-line (EOL) resistors must be removed from the control panel.

Also, do not enable any POPIT points (or OctoPOPIT points) sharing the same point number as the Door point. Failure to do so results in extra point trouble conditions upon reboot.

D# Interlock Point

Default:	Blank
Selection:	Blank, 1 to 127, 129 to 247
1 to 127, 129 to 247	The point number assigned to the Interlock point. Points 128 and 248 are reserved by the control panel for internal use.
Blank	No point number is assigned to the Interlock point.

Enter the interlock point number. This point, when faulted, prevents the door controller from allowing access upon a valid ID read or door request.

Do not assign this point to another **D# Door Point**. You can, however, assign it to another controller to prevent multiple controllers from activating.



Door points must be programmed as Perimeter points. If a 24-hour point type is required for the Door point, you can use a Perimeter point type with a Point Response of 9 to C. Also, the debounce count must be set to 4 in Point Assignments.



The Interlock point is considered in a normal state if it is bypassed, swinger bypassed, or forced armed. This results in normal access even if the door remains open.

D# Auto Door?

Default:	No
Selection:	Yes or No
Yes	When the area assigned in D# Entry Area # is disarmed, the door is in the unlocked state. When that area is armed, the door returns to the locked state.
No	Door state is not affected by the armed state of the area.

Use this program item to automatically unlock the door (latched, shunt, and strike) when the entry area is disarmed. The door re-locks upon Master or Perimeter Arming the area.



The unlocked state cannot be overridden manually.

D# Fire Unlock?

Default:	No
Selection:	Yes or No
Yes	Relay activates and shunt is applied for the door contact automatically upon a Fire Alarm.
No	Door remains in its current mode upon a Fire Alarm.

Use this program item to activate the relay for the door strike and shunt the door zone automatically upon a Fire Alarm. This feature overrides a Secure Door state, Locked Door state, Auto Door, and an Interlock Faulted point. The relay activates for all doors with this prompt programmed as **Yes** when a Fire Alarm occurs in any area. Relays that are activated by Fire Unlock can be returned to normal only through the keypad using the Door Control function.



Doors that are activated by Fire Unlock must be returned to normal using the Door Control function on the keypad.



This command unlocks the door regardless of the armed state.



Each fire alarm that is generated causes a Door Unlocked – Automatic Event.

D# Disarm on Open?

Default:	Yes
Selection:	Yes or No
Yes	The area disarms only after the door is opened for a user with a valid disarm level.
No	The area disarms whether or not the door is opened as soon as a user with a valid disarm level presents a valid token or card.

Use this program item to determine if the door needs to be physically opened before disarming the area upon a valid access request. The user initiating the access request needs access levels that allow disarming with ID.

D# Card Type

Default:	0
Selection:	0 to 3
0	Card format is 26-bit Wiegand.
3	Do not use. Card format is 37-bit fidelity.

This item must be kept to a value of 0 (26 bit Wiegand format).

7.2 Strike Profile

This programming category is used to create a specific door profile for:

- Strike and shunt times.
- Extending strike and shunt times if a door is left open.
- Resetting the strike when the door opens.

Door

Default: 1
Selection: 1 to 8

Enter the door you are programming.

D# Strike Time

Default: 10 sec	
Selection: 1 sec to 240 sec	
Blank	Strike Time is not programmed for this door.
1 to 240	The strike activates for the amount of time programmed.

Enter the amount of time the door controller toggles the relay output to activate the door strike. When the door strike is activated, the user can open the door. The strike activates for a valid token, RTE, REX, and the keypad CYCLE DOOR? function.

D# Shunt Time

Default: 10 sec	
Selection: Blank, 1 sec to 240 sec	
Blank	Shunt Time is not programmed for this door.
1 to 240	The shunt activates for the amount of time programmed.

Enter the amount of time that the Door point is shunted to allow a user to open the door. The duration of time should be sufficient so that the opened door does not cause the point to enter into a trouble, alarm, or faulted condition.

D# Buzz Time

Default: 2 sec	
Selection: Blank, 1 sec to 240 sec	
Blank	Buzz Time is not programmed for this door.
1 to 240	The buzzer sounds for the amount of time programmed.

Enter the amount of time the buzzer output sounds to notify the user that the strike was activated and the door is ready to open. The buzzer stops as soon as the door is opened.



A separate buzzer is required. Many readers have an internal buzzer that is not affected by Buzz Time.

D# Extend Time

Default: 10
Selection: Blank, 1 sec to 30 sec

Enter the amount of time that strike, buzz, and shunt activation is prolonged if a door is left open and the shunt time expires. At the end of the programmed extend time, the buzzer continues to buzz until the door closes. If programmed, the point assigned to the door indicates a trouble, alarm, or fault at the keypad.



The CLOSE DOOR # display on keypad does not activate if no time (blank) is programmed.



Regardless of how the Door point is programmed, the system generates a Trouble Door Left Open Event while the system is disarmed, and an Alarm Door Left Open Event if the system is armed and the door is held open beyond Extend Time. Door Closed - Restoral Events are generated after the door is held open past Extend Time and the door returns to normal.

D# Deact On Open?

Default:	Yes
Selection:	Yes or No
Yes	Strike deactivates when the door is opened after a valid Access Granted request.
No	Strike remains activated for the amount of the programmed strike time whether door is opened or closed.

Determines if the strike deactivates immediately upon physically opening the door.



In order for this function to work, a point needs to be assigned to the door.



To Reduce False Alarms, maintain **D# Deact on Open?** as the default (**Yes**). This helps prevent the door from bouncing open and causing a false alarm.

D# RTE Shunt Only?

Default:	No
Selection:	Yes or No
Yes	Programmed shunt time activates so door can be manually opened.
No	RTE automatically activates the programmed strike and shunt time.

Use this program item to disable the strike, but still activate the programmed shunt time at a Request to Enter (RTE) area.



Use this parameter when a user can open a door manually without relying on a token or card to activate the strike (such as with a push bar).



When **RTE Shunt Only** is Yes, RTE Events are not logged, reported, or printed.

D# REXShunt Only?

Default:	No
Selection:	Yes or No
Yes	Programmed shunt time activates so the door can be manually opened.
No	REX automatically activates the programmed strike and shunt time.

Use this program item to disable the door strike, but activate the programmed **D# Shunt Time** upon a request to exit (REX) from an area.



Use this parameter when a user can open a door manually without relying on a token or card to activate the strike (such as with a push bar).



When **REXShunt Only** is Yes, REX Events are not logged, reported, or printed.

7.3 Event Profile

This programming category is used to determine if events are created for:

- Access Granted and Access Denied
- Door Requests
- Door state changes due to manual (keypad) or automatic scheduled or armed state changes (skeds/hold open on disarm, normal on armed) operation.

Door #

Default:	1
Selection:	1 to 8

Enter the door you plan to program.



RTE Events require **Access Granted** to be programmed as **Yes**.

D# Access Granted?

Default:	No
Selection:	Yes or No
Yes	Access Events from this door controller are sent to the control panel for processing.
No	Access Events from this door controller are not sent to the control panel for processing.

This program item determines if Access Granted and Door Request Events are sent to the control panel for processing memory, printing, and remote reporting.



A successful Access Event can be started by a(n):

- Valid user ID
- Valid door state changed at the keypad.
- Automatically scheduled or armed state change that holds a door open
- RTE or REX.

D# No Entry?

Default:	No
Selection:	Yes or No
Yes	Access Denied Events from this door controller are sent to the control panel for processing.
No	Access Denied Events from this door controller are not sent to the control panel for processing.

This program item determines if No Entry Events are sent to the control panel for processing memory, printing, and remote reporting.



A No Entry Event can be caused by:

- Invalid or unknown user ID, interlock or secured door, or incorrect authority level
- RTE or REX at an interlocked door.
- RTE or REX at a door in the secured mode.

D# Enter Request?

Default:	No
Selection:	Yes or No
Yes	A Door RTE Event from this door controller is sent to the control panel for processing.
No	A Door RTE Event from this door controller is not sent to the control panel for processing.

This program item determines if RTE Events are sent to the control panel for processing memory, printing, and remote reporting.



RTE Events require **D# Access Granted** to be programmed as **Yes**.

D# Exit Request?

Default:	No
Selection:	Yes or No
Yes	A Door REX Event from this door controller is sent to the control panel for processing.
No	A Door REX Event from this door controller is not sent to the control panel for processing.

This program item determines if REX Events are sent to the control panel for processing memory, printing, and remote reporting.



REX Events require **D# Access Granted** to be programmed as **Yes**.

8.0 SIA CP-01 Quick Reference

Table 45: Programming the Control Panels for SIA CP--01 Compliance

Prompt Name	Bosch Recommended Settings for SIA CP-01 Compliance	Shipping Default	References
Phone #	(Prefix backup phone number with Call Waiting disable command)	{Blank}	Page 11
Duress Type	Option 3	0 (disabled)	Page 35
Cancel Report	Yes	Yes	Page 36
A# Exit Dly Time	45 sec to 255 sec	60 sec	Page 38
A# Duress Enable	Yes	No	Page 39
A# Exit Restart	Yes or No	Yes	Page 49
A# Arm No Exit	Yes or No	Yes	Page 49
A# Two Man Rule	No	No	Page 47
A# Early Ambush	No	No	Page 48
A# Exit Warning	Yes	Yes	Page 49
A# Entry Warning	Yes	Yes	Page 49
A# Burg Time¹	6 min to 90 min	6 min	Page 42
A# Alarm Bell	1 to 128(64), A, B, C	A (on-board alarm output)	Page 79
CC# Entry Tone	Yes or No	Yes	Page 54
CC# Exit Tone	Yes or No	Yes	Page 54
CC# Abort Display	Yes or No	Yes	Page 56
CC# Cancel Display	Yes or No	Yes	Page 56
Master Arm Inst	{Blank}	{Blank}	Page 61
Perim Instant	{Blank}	{Blank}	Page 61
L## Send Duress	[Blank] or E	E ²	Page 75
L## Disarm	[Blank] or E	E ²	Page 67
L## Passcode Disarm	[Blank] or E	E ²	Page 75
P## Entry Delay	30 sec to 240 sec	30 sec	Page 92
P## Alarm Abort	Yes or No	Yes ³	Page 101
Abort Window	15 sec to 45 sec	30 sec	Page 141
Passcode Length	3 to 6 digits	Disabled	Page 141
Swinger Count	1 to 2 trips	1 trip	Page 141
Remote Warning	Yes	Yes	Page 142
Cross Point Time	5 to 255 sec	20 sec	Page 143
P## Cross Point	Yes or No	No	Page 99

¹ The SIA allowed range is 1 min to 90 min. Must additionally comply with UL requirements, refer to section *A# Burg Time*.

² L14 is the default duress user index.

³ The default for P## Alarm Abort is **No** for P3, P4, P5, and P22.

Programming Prompts Directory

GV2MAIN	11	AC Fail Time	28
Phone	11	AC Fail Display	29
Phone 1	11	AC Fail/Res Rpt.....	29
Phone 2	12	AC Tag Along	30
Phone 3	12	AC/Battery Buzz	30
Phone 4	12	Bat Fail/Res Rpt	30
Phone Parameters.....	12	Printer Parameters	30
Modem Format.....	12	Printer Address.....	30
Point/User Flag	13	P### Area Assign.....	102
DTMF Dialing	14	P## Supervised	31
Phone Supv Time	14	P## Scope.....	31
Alarm On Fail	14	P## A1 [through A8] in Scope	31
Buzz on Fail	15	P## Fire Events	32
Two Phone Lines	15	P## Burglar Event	32
BFSK Duress Code.....	15	P## Access Event	32
Expand Test Rpt	15	P## User Event	32
Routing.....	16	P## Test Event.....	32
<i>Dialing Attempts.....</i>	<i>17</i>	P## Diag Event	32
Route #	17	P## Auto Functions Event.....	32
R# Primary Device	17	P## RPS Event	32
R# Backup Device	17	P## Relay Event.....	32
View Events?	17	P## Point Event.....	32
Fire Reports.....	18	P## Usr Chng Evt.....	32
Burglar Reports	18	RPS Parameters.....	32
User Reports	18	<i>RPS Callback Reports</i>	<i>33</i>
Test Reports.....	14	RPS Passcode	33
Diag Reports	20	Log % Full	33
Relay Reports.....	21	RPS Call Back.....	34
AutoFunc Reports.....	21	RPS Line Monitor	34
RPS Reports	21	Answer Armed.....	34
Point Reports	22	Answer Disarmed	34
User Chng Reports.....	23	RPS Ph	34
Access Reports	23	Miscellaneous	35
Enhanced Routing	24	Duress Type.....	35
<i>Programming a Duplicate Report</i>	<i>24</i>	Cancel Report	36
RG# Primary SDI 88	25	Area Parameters	36
RG# Backup SDI 88.....	25	Area	36
RG# Primary SDI 92	25	A# Area On	36
RG# Backup SDI 92.....	25	A# Acct Number	36
RG# Primary Pager.....	25	A# FA Bypass Max.....	37
Power Supervision.....	28		

A# Delay Res	37	CC# Trouble Tone	53
A# Exit Tone	38	CC# Entry Tone	54
A# Exit Dly Time	38	CC# Exit Tone	54
A# Auto Watch	38	CC# Arm Now Warn	54
A# Verify Time	38	CC# Close Door	54
A# Duress Enable	39	CC# EnhancCmdCtr	54
A# Area Type	40	CC# Passcode Follows Scope	55
<i>Bell Parameters</i>	41	CC# Scroll Lock	55
Area	42	CC# Menu Key Lock	55
A# Fire Time	42	CC# Abort Display	56
A# Fire Pat	42	CC# Cancel Display	56
A# Burg Time	42	<i>Area Text</i>	56
A# Burg Pat	42	Area	56
A# Single Ring	43	Area# Is On	56
A# Bell Test	43	Area# Not Ready	56
<i>Open/Close Options</i>	43	Area# Is Off	56
Area	44	Area# Acct Is On	56
A# Acct O/C	44	<i>Custom Function</i>	57
A# Area O/C	45	Custom Function	57
A# Disable O/C in Window	45	CF### Text	57
A# Auto Close	45	CF### Key Strokes	58
A# Fail to Open	45	User Interface	60
A# Fail to Close	46	<i>Keypad Selections</i>	60
A# Restrictd O/C	46	Master Arm Delay	61
A# Perimeter O/C	47	Mstr Arm Inst	61
A# Latest Close Time	44	Perim Instant	61
<i>Arming Features</i>	47	Perim Delay	61
A# Two Man Rule	47	Watch Mode	61
A# Early Ambush	48	Perim Partial	62
A# Exit Restart	49	View Area Stat	62
A# Arm No Exit	49	View Memory	62
A# Exit Warning	49	View Pt Status	62
A# Entry Warning	49	Walk Test	62
Keypad (Command Center)	50	Fire Test	62
<i>Keypad (Command Center) Assignment</i>	50	Send Report	63
Cmd Center	50	<i>Access Control Functions</i>	63
CC# Supervised	51	Door Control	63
CC# Area Assign	51	Access Ctl Level	63
CC# Scope	51	Chg Display	63
CC# A1 [through A8] in Scope	51	Chg Time/Date	63
CC# Entr Key Rly	52	Chg Passcode	63
CC# Entr Cycl Dr	52	Add User	64
CC# Assign Door	53	Del User	64

Extend Close	64	L## View Log	72
View Log	64	L## Print Log.....	72
Print Log	64	L## User Cmd 7	72
User Cmd 7.....	64	L## User Cmd 9	72
User Cmd 9.....	65	L## Bypass a Pt.....	72
Bypass a Pt.....	65	L## Unbypass a Pt.....	73
Unbypass a Pt.....	65	L## Reset Sensors.....	73
Reset Sensors	65	L## Change Relay.....	73
Change Relay	65	L## Remote Program	73
Remote Program.....	65	L## Move to Area.....	73
Move to Area	66	L## Display Rev	73
Display Rev.....	66	L## Service Walk	73
Service Walk.....	66	L## Default Text.....	74
Default Text	66	L## Change Skeds.....	74
Change Skeds	66	L## Invisible Walk Test	74
Invisible Walk Test.....	66	<i>Custom Functions</i>	<i>75</i>
C Function 128 [through 143].....	67	L## C Function 128 [through 143]	75
<i>Authority Level Selections</i>	<i>67</i>	L## Force Arm.....	75
Authority Level	67	L## Area O/C	75
L## Disarm	67	L## Restricted O/C.....	75
L## Master Arm Delay	68	L## Perimeter O/C	75
L## Mstr Arm Inst		L## Send Duress.....	75
L## Perim Instant.....	68	L## Passcode Arm	75
L## Perim Delay	68	L## Passcode Disarm	75
L## Watch Mode.....	68	<i>Access Control Levels</i>	<i>75</i>
L## Perim Partial	68	L## Security Level.....	75
L## View Area Stat	68	L## Disarm Level	76
L## View Memory	69	L## Function Level	76
L## View Pt Status.....	69	Function List.....	77
L## Walk Test.....	69	Menu Item	77
L## Fire Test.....	69	M## Function	77
L## Send Report.....	70	M## CC Address 1 [through 8]	78
L## Door Control.....	70	Relay Parameters	78
L## Cycle Door.....	70	Area Relays.....	79
L## Unlock Door.....	70	Area	79
L## Secure Door	70	A# Alarm Bell	79
L## Access Ctl Lvl	71	A# Fire Bell.....	79
L## Chg Display.....	71	A# Reset Sensors	79
L## Chg Time/Date.....	71	A# Fail to Close	80
L## Chg Passcode.....	71	A# Force Armed	80
L## Add User.....	71	A# Watch Mode.....	80
L## Del User.....	72	A# Area Armed.....	80
L## Extend Close.....	72	A# Area Fault	80

A# Duress Relay.....	81	P## Local While Disarmed	96
A# Perim Fault	81	P## Local While Armed	97
A# Silent Alarm	81	P## Disable Rst.....	97
<i>Panel-Wide Relays</i>	<i>81</i>	P## FA Retrnable.....	97
AC Failure.....	81	P## BP Retrnable.....	98
Battery Trouble	81	P## Bypassable	98
Phone Fail.....	81	P## Swinger Byps	99
Comm	82	P## Report Bypass at Occurrence	99
Log % Full.....	82	P## Defer BP Report.....	99
Summary Fire	82	P## Cross Point	99
Summary Alarm	82	P## Fire Point	100
Summary Fire Tbl	82	P## Alarm Verify	100
Summary SupFire	82	P## Resettable.....	100
Summary Trouble	82	P## Alarm Abort.....	101
Summary SupBurg.....	82	Point Assignments	101
RADXUSR1/RADXUSR2	82	Point Number	101
Passcode or Token Worksheet.....	82	P### Point Index.....	101
<i>Reporting and Logging</i>	<i>84</i>	P### Area Assign.....	102
User ###	84	P### Debounce.....	102
U### Passcode.....	85	P### BFSK/Relay	102
U### User Group.....	85	P### Point Text.....	103
U### Area 1 [through Area 8] Auth	85	COMMAND 7 and COMMAND 9.....	103
U### Name.....	86	CMD7 Point Index	103
U### Mstr Site	86	CMD7 BFSK/Relay.....	103
U### Mstr Crd Data	86	CMD7 Point Text.....	103
U### SU1 through SU3 Site	86	CMD9 Point Index	104
U### SU1 through SU3 C/D	86	CMD9 BFSK/Relay.....	104
RADXPNTS	87	CMD9 Point Text.....	104
Point Index.....	87	RADXSKE.....	105
Point Index.....	87	Windows	105
P## Type	87	<i>Opening and Closing.....</i>	<i>105</i>
Point Responses	91	Window	105
P## Pt Response	92	W# Sunday.....	105
P## Entry Delay	92	W# Monday	106
P## Ent Tone Off	93	W# Tuesday	106
P## Silent Bell	93	W# Wednesday	106
P## Ring Til Rst.....	93	W# Thursday	106
P## Audible After 2 Failures	94	W# Friday.....	106
P## Invisible Pt.....	94	W# Saturday	106
P## Buzz On Fault.....	95	W# Open Early Begin.....	106
P## Watch Point	96	W# Open Window Start.....	107
P## RlyResp Type	96	W# Open Window Stop	107
P## Disp as Dvc	96	W# Close Early Begin	108

W# Close Window Start	109	S## Door 1 [through 8].....	120
W# Close Window Stop	109	S## Door 1 [through 8].....	120
W# Xept Holiday	110	S## Door 1 [through 8].....	121
W# Holiday 1	110	S## Door 1 [through 8].....	121
W# Holiday 2	110	S## Door 1 [through 8].....	121
W# Holiday 3	110	S## Time.....	122
W# Holiday 4	110	S## Date	122
W# Area 1 [through 8].....	110	S## Sunday.....	122
<i>User Group Windows</i>	112	S## Monday.....	122
User Windows #.....	112	S## Tuesday.....	122
UW# User Group	112	S## Wednesday.....	122
UW# Sunday.....	113	S## Thursday.....	122
UW# Monday	113	S## Friday.....	122
UW# Tuesday.....	113	S## Saturday	122
UW# Wednesday.....	113	S## Xept Holiday.....	123
UW# Thursday.....	113	S## Holiday 1.....	123
UW# Friday.....	113	S## Holiday 2.....	123
UW# Saturday.....	113	S## Holiday 3.....	123
UW# Group Enable.....	113	S## Holiday 4.....	123
UW# Group Disable	113	Holiday Indexes	123
<i>Holiday Indexes for User Group Windows</i>	114	<i>Add/Change/Delete</i>	123
UW# Xept Holiday.....	114	Date	123
UW# Holiday 1 [through 4].....	114	Holiday Index 1.....	123
Skeds	114	Holiday Index 2.....	124
Sked Number	114	Holiday Index 3.....	124
S## TimeEdit	114	Holiday Index 4.....	124
S## Function Code	114	<i>View Holidays</i>	124
S## Area 1[through 8]	115	Index 1 Days	124
S## Area 1[through 8]	115	Index 2 Days	124
S## Point Number	115	Index 3 Days	124
S## Point Number	115	Index 4 Days	124
S## Area 1[through 8]	116	GV2AUX	124
S## Relay Number	116	SDI Automation	125
S## Relay Number	116	Enable SDI Auto.....	125
S## Defer Test	117	Baud Rate	125
S## Hourly Report.....	117	Parity/Stop.....	125
S## Defer Status	117	Supervise SDI 80	125
S## Cmd Center.....	118	RTS Control	125
S## Custom Func.....	118	DTR Control	126
S## Cmd Center 1[through 8]....	119	Status Rate	126
S## Access Ctl Level #.....	119	SDI RPS Parameters	126
S## Access Ctl Level #.....	119	<i>User Interface Modifications for COMMAND 43</i>	127
S## Door 1 [through 8]	120		

Enable SDI RPS	127	Secondary Ambush Code.....	140
Call Back Enabled.....	127	Abort Window.....	141
RPS IP Address 1	129	Passcode Length.....	141
RPS IP Address 2	129	Swinger Count.....	141
RPS IP Address 3	129	Remote Warning	142
RPS IP Address 4	129	Perimeter Relay.....	142
RPS Port Number	129	Early Armed Relay	142
<i>Using an External Modem</i>	<i>129</i>	Cross Point Parameters.....	142
Enable Ext Modem.....	133	Cross Point Time	143
Answer Armed	133	RADXAXS.....	144
Answer Disarmed.....	133	Door Profile	144
RPS Line Monitor.....	133	Door #	144
Seize Relay.....	133	D# Entry Area #.....	144
Modem Init String.....	133	D#CC#Scope	144
RPS Dial String	133	D# Custom Function.....	144
Programming Path Numbers and IP		D# Door Point.....	145
Addresses for Enhanced Communications		D# Interlock Point.....	145
.....	134	D# Auto Door?	146
Enhanced Comm	134	D# Fire Unlock?.....	146
Path # IP Add1.....	134	D# Disarm on Open?.....	146
Path # IP Add2.....	134	D# Card Type.....	146
Path # IP Add3.....	134	Strike Profile	147
Path # IP Add4.....	135	Door #	147
Path # PortNum	135	D# Strike Time.....	147
Path # Poll Rate	135	D# Shunt Time	147
Path # Ack Wait	137	D# Buzz Time.....	147
Path # Retry Count	137	D# Extend Time.....	147
Path # Anti-Replay	138	D# Deact On Open?	148
SDI RPS/Enhanced Communications		D# RTE Shunt Only?	148
Configuration.....	138	D# REXShunt Only?.....	148
Baud Rate.....	138	Event Profile.....	148
Parity/Stop	138	Door #	148
RTS Control	138	D# Access Granted?	149
DTR Control.....	138	D# No Entry?.....	149
Supervise SDI 88	139	D# Enter Request?	149
Supervise SDI 92	139	D# Exit Request?	149
Route Group	139		
RG# 1 Faster Rate	139		
Miscellaneous.....	139		
Fire Summary Sustain	139		
Fire Supv Res Type	140		
Enable Protocol Type.....	140		
Fire Trouble Resound	140		
Early Ambush Timer	140		

Notes

Bosch Security Systems, Inc.
130 Perinton Parkway
Fairport, NY, 14450
USA
www.boschsecurity.com

© Bosch Security Systems, Inc., 2010
F01U143071-02



BOSCH