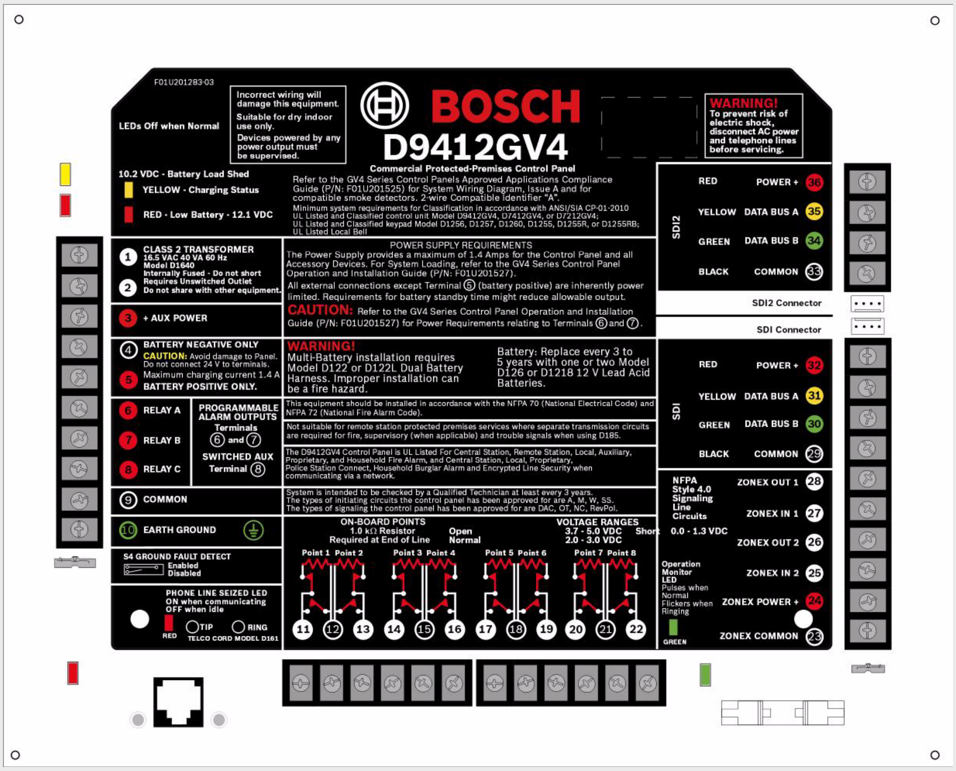


# D9412GV4/D7412GV4/D7212GV4

## Control Panels

**en** Program Entry Guide

# Table of Contents

**1 System Requirements 6**

**2 Introduction 7**
2.1 Using this Program Entry Guide 7
2.2 Guide to UL 864 Programming Requirements for D9412GV4 and D7412GV4 Control Panels 7
2.3 Guide to UL 636 Programming Requirements for D9412GV4/ D7412GV4/D7212GV4 Control Panels 10
2.4 Guide to Programming Descriptions 11
2.5 Guide to Keypad Tools 11
2.5.1 Keypad Programming Menu 12
2.5.2 Service Bypass Menu 14
2.5.3 RF Points Menu 14
2.5.4 RF Repeaters Menu 15
2.5.5 RF Diagnostics Menu 15
2.5.6 IP Diagnostics Menu 16

**3 Panel and Area Wide Parameters 17**
3.1 Phone 17
3.2 Phone Parameters 19
3.2.1 Special Point/User Reporting 21
3.3 Routing 23
3.3.1 Call Party Disconnect 24
3.3.2 Route Number Groups: Which Has the Highest Priority? 24
3.3.3 Programming Primary and Backup Destinations 24
3.3.4 Enhanced Routing 24
3.3.5 Programming a Duplicate Report 25
3.3.6 Routing Destination Communication Failures 25
3.3.7 Message Prioritization within a Route Number 25
3.3.8 Route Group Parameters 29
3.3.9 Communication Attempts 30
3.3.10 Route Group Categories 33
3.4 Programming Path Numbers and Network Addresses for Enhanced Communications 40
3.4.1 Anti-Replay Security Feature 45
3.5 SDI RPS/Enhanced Communications Configuration 45
3.5.1 Configuration for RPS Over Network 46
3.6 Power Supervision 50
3.7 Printer Parameters 52
3.8 RPS Parameters 54
3.8.1 Uploading and Downloading Reports 54
3.8.2 Log Threshold Reports 54
3.8.3 Panel Initiated Unattended RPS 55
3.9 Miscellaneous 59
3.10 Area Parameters 61
3.10.1 Area Parameters 61
3.10.2 Shared-Area Characteristics 65
3.10.3 Bell Parameters 66
3.10.4 Open/Close Options 69

3.10.5 Arming Features 74
3.11 Keypad (Command Center) 78
3.11.1 Keypad (Command Center) Assignment 79
3.11.2 Area Text 88
3.11.3 Custom Function 89
3.12 User Interface 93
3.12.1 Commands 93
3.12.2 Command Authorization 93
3.12.3 Access Control Functions 96
3.12.4 Custom Functions 101
3.12.5 Configuration Authority 101
3.12.6 Authority Level Selections 102
3.12.7 General Functions 108
3.12.8 Report Levels 113
3.12.9 Access Control Levels 114
3.12.10 SIA Duress Passcode Options 116
3.13 Function List 116
3.14 Relay Parameters 117
3.14.1 Area Relays 118
3.14.2 Panel-Wide Relays 121
3.14.3 Relay/Output Configuration 124

**4 Passcodes, Access Credentials, and User Groups 125**
4.1 Passcode or Token Worksheet 125
4.1.1 User Credentials 125
4.1.2 Passcodes 125
4.1.3 User Group Window 125
4.1.4 User Name 125
4.1.5 Tokens and Cards 126
4.1.6 Reporting and Logging 126

**5 Points 130**
5.1 Point Index 130
5.2 Point Responses 132
5.2.1 Applications for Point Responses 9, D, and E: 132
5.2.2 Characteristics of a Fire Point: 133
5.3 Point Assignments 146
5.4 Cross Point Parameters 149
5.5 COMMAND 7 and COMMAND 9 151

**6 Schedules (Skeds) 154**
6.1 Windows 154
6.1.1 Opening and Closing 154
6.1.2 User Group Windows 162
6.1.3 Holiday Indexes for User Group Windows 164
6.2 Schedules (Skeds) 164
6.3 Holiday Indexes 173

**7 AUXPARM 174**
7.1 Automation 174
7.2 Miscellaneous 175

**8 SDI2 Modules 179**
8.1 B208 Octo-input Module 179
8.2 B308 Octo-output Module 179
8.3 B420 Ethernet Communication Module 179
8.3.1 IP Diagnostics Keypad Menu (B420) 189
8.4 B820 SDI2 Inovonics Interface Module 190
8.5 Wireless Repeater 190
8.5.1 RF Repeaters Keypad Menu (RFID Wireless Repeaters) 191
8.5.2 RF Diagnostics Keypad Menu (RFID Wireless Repeaters) 193

**9 ACCESS CONTROL (D9412GV4/D7412GV4) 195**
9.1 Door Profile 195
9.2 Strike Profile 198
9.3 Event Profile 200

**10 SIA CP-01 Quick Reference 203**

**11 Keypad Tools Menu (Options Not Available in RPS) 204**
11.1 Service Bypass Menu 204
11.1.1 Setting Service Bypass (PT NUM 1-247) 204
11.1.2 Resetting Service Bypass 204
11.2 RF Points Menu 205
11.2.1 Enroll RF Point 205
11.2.2 Replace RF Point 205
11.2.3 Remove RF Point 206

# 1 System Requirements

⚠ **WARNING!**

Minimum system requirements for Classification in accordance with ANSI/SIA CP-01-2007: UL Listed and Classified control unit Model D9412GV4 or D7412GV4 or D7212GV4.

UL Listed and Classified keypad Model D1256, D1257, D1260, D1255, D1255R, or D1255 RW.

UL Listed Local Bell.

| **Control Panel** | **Firmware Version** |
|---|---|
| D9412GV4 | 1.00 or later |
| D7412GV4 | 1.00 or later |
| D7212GV4 | 1.00 or later |

# 2 Introduction

## 2.1 Using this Program Entry Guide

This guide is for programming the GV4 Series Control Panels.

| Features | D9412GV4 | D7412GV4 | D7212GV4 |
|---|---|---|---|
| Access Control | Eight Doors | Two Doors | N/A |
| Passcodes | 999 | 399 | 99 |
| Cards/tokens | 999 | 399 | N/A |
| Passcode-protected custom functions | 16 | 4 | 4 |
| Number of printers | 3 | 1 | 1 |
| Number of points | 246 | 75 | 40 |
| Number of off-board relays | 128 | 64 | 24 |
| Areas | 32 | 8 | 4 |

| Document Name | Part Numbers |
|---|---|
| D1255 Installation Instructions | 74-06819-000 |
| D1256/D1257 Installation Instructions | 74-06925-000 |
| D1255RB/D1256RB/D1257RB Installation Instructions | F01U011791 |
| D1260 Installation Guide | 48101 |
| D1260 Owner’s Manual | 50410 |
| D6500 Report Directory | 74-04651-001 |
| Conettix D6600/6100 Receiver/Gateway Program Entry Guide | 4998122702 |
| Conettix D6600/6100 Receiver/Gateway Computer Interface Manuals | 4998122703 |
| D720 Series Installation Guide | 74-06918-000 |
| D9210C Operation and Installation Guide | F01U215244 |
| D9210C Program Entry Guide | F01U201526 |
| D9412GV4/D7412GV4/D7212GV4 Installation and Operation Guide | F01U201527 |
| D9412GV4/D7412GV4/D7212GV4 Program Record Sheet | F01U214958 |
| RPS Installation Guide | 4998141259 |

**Table 2.1** Referenced Literature

## 2.2 Guide to UL 864 Programming Requirements for D9412GV4 and D7412GV4 Control Panels

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

**NOTICE!**

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 2.2, Page 10*.

| 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 | *17* |
| Phone Supervision | Yes | 0 to 240 sec | 10 to 200 sec | *22* |
| Alarm On Fail | No | Yes / No | Set to **No** | *22* |

| **Product Feature/ Option** | **Permitted in UL 864? (Y/N)** | **Possible Settings** | **Settings Permitted in UL 864** | **Refer to Page:** |
|---|---|---|---|---|
| Two Phone Lines | Yes | Yes / No | Set to **Yes** when using PSTN communications | *23* |
| Expand Test Report | Yes | Yes/No | Set to **Yes** | *23* |
| Fire Reports | Yes | Yes / No | Set to **Yes** | *33* |
| R# Fire Supervisory Missing | Required | Yes/No | Set to **Yes** | *35* |
| Test Reports | Yes | Yes / No | Set to Yes | *35* |
| AC Fail Report | Yes | Yes / No | Set to Yes | *51* |
| AC Restoral Report | Yes | Yes / No | Set to Yes | *51* |
| Battery Missing Report | Yes | Yes / No | Set to Yes | *37* |
| Low Battery Report | Yes | Yes / No | Set to Yes | *37* |
| Battery Restoral Report | Yes | Yes / No | Set to Yes | *51* |
| AC Fail Time | Yes | 1:00 to 90:00 min | Enter 1:00 | *50* |
| AC Fail Display | Yes | 10 to 300 sec | 10 to 200 sec | *50* |
| AC Tag Along | Yes | Yes / No | Set to Yes | *51* |
| AC/Battery Buzz | Yes | Yes / No | Set to Yes | *51* |
| Bat Fail/Restoral Report | Yes | Yes / No | Set to Yes | *51* |
| R# Service Start Report | Required | Yes / No | Set to Yes | *39* |
| R# Service End Report | Required | Yes / No | Set to Yes | *39* |
| R# Fire Walk St Report | Required | Yes / No | Set to Yes | *39* |
| R# Fire Walk End Report | Required | Yes / No | Set to Yes | *39* |
| R# Walk Test St Report | Required | Yes / No | Set to Yes | *39* |
| R# Walk Test End Report | Required | Yes / No | Set to Yes | *39* |
| AC Fail Time | Yes | 1:00 to 90:00 min | Enter 1:00 | *50* |
| AC Fail Display | Yes | 10 to 300 sec | 10 to 200 sec | *50* |
| AC Tag Along | Yes | Yes / No | Set to Yes | *51* |
| AC/Battery Buzz | Yes | Yes / No | Set to Yes | *51* |
| Bat Fail/Restoral Report | Yes | Yes / No | Set to Yes | *51* |
| Area 1 Area On | Required to send system status reports | Yes / No | Set to Yes | *61* |
| A# Delay Restoral | Yes | Yes / No | Set to Yes | *62* |
| Verify Time | Yes | 10 to 60 sec | 60 sec | *63* |
| Area # Fire Time | Yes | 1 to 90 min | 5 min (check with AHJ) | *67* |
| CC# Supervised | Yes | Yes / No | Set to Yes | *79* |
| CC# Trouble Tone | Yes | Yes / No | Set to Yes | *85* |
| CC# Scroll Lock | Yes | Yes / No | Set to Yes | *87* |

| **Product Feature/ Option** | **Permitted in UL 864? (Y/N)** | **Possible Settings** | **Settings Permitted in UL 864** | **Refer to Page:** |
|---|---|---|---|---|
| Remote Program | Disable / Enable | -, E, or P | Set to P | *100* |
| A# Fire Bell | Yes | 0 to 128, A, B, C0 to 128, A, B, C | Program with a relay | *118* |
| A# Reset Sensors | Yes | | Program with a relay | *119* |
| U### Area # Auth | Yes | 0 to 8 | Program an Authority Level for the Fire Area | *127* |
| U### Passcode | Yes | 3-, 4-, 5-, or 6-digit passcode | Must program at least one passcode | *126* |
| P## Silent Bell | No | Yes / No | Set to No | *135* |
| P## Invisible Point | No | Yes / No | Set to No | *136* |
| P## Local While Disarmed | No | Yes / No | Set to No | *139* |
| P## Local While Armed | No | Yes / No | Set to No | *139* |
| P## Disable Restorals | No | Yes / No | Set to No | *140* |
| P## Bypassable | No | Yes / No | Set to No | *141* |
| P## Swinger Bypass | No | Yes / No | Set to No | *142* |
| P## Fire Point | Yes | Yes / No | Set to Yes | *143* |
| P## Resettable | Yes | Yes / No | As required | *144* |
| Sked## Function Code | Required | 1 to 11, 13 to 28 | Sked Function Code 9 | *165* |
| Sked## Defer Test | No | Yes / No | Set to No | *165* |
| Sked## Hourly Test(Report?) | No | Yes / No | Set to No | *165* |
| Sked## Time | Enter valid time | 00:00 to 23:59 | 00:00 to 23:59 | *171* |
| Sked## Date | No | mm/dd | Set to No | *171* |
| Sked## Sunday | Yes | Yes / No | Set to Yes | *171* |
| Sked## Monday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Tuesday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Wednesday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Thursday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Friday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Saturday | Yes | Yes / No | Set to Yes | *172* |
| Sked## Xept On Holiday | No | Yes / No | Set to No | *172* |
| | | | | |
| **For IP Communications to a D6600 Receiver** | | | | |
| Enhanced Comm | Yes | Yes / No | Set to Yes | *40* |
| Path1 IP Add1 (2, 3 or 4) | Yes | 000 to 255 | Program a valid IP address | *41* |
| Path 1 Poll Rate | Yes | 0, 5 to 65535 sec* | Program as necessary | *41* |
| Path 1 Ack Wait | Yes | 0, 5 to 65535 sec* | Program as necessary | *45* |

| **Product Feature/ Option** | **Permitted in UL 864? (Y/N)** | **Possible Settings** | **Settings Permitted in UL 864** | **Refer to Page:** |
|---|---|---|---|---|
| Path 1 Retry Count | Yes | 0 to 255 | Program as necessary | *45* |
| | | | | |
| **For Ground Fault Enable Switch** | | | | |
| (Refer to the *D9412GV4/ D7412GV4/ D7212GV4 Operation and Installation Guide* (P/N: F01U201527) | Yes | Closed = Enabled<br>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.

| **Prompt** | **Possible Settings** | **Recommendations** |
|---|---|---|
| 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# Enhanced CommandCenter | 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 | 0 to 8 | Program as 0 |
| P## Ring Until Restored | 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 |

**Table 2.2** UL 864 Programming Requirements

## 2.3 Guide to UL 636 Programming Requirements for D9412GV4/ D7412GV4/D7212GV4 Control Panels

When using a D9412GV4/D7412GV4/D7212GV4 control panel for hold-up operation, a hold-up point should have the following setting applied to it:

– P## Type = 0 (Point is constantly armed regardless of the status of the system.)

- P## Invisible Point = Yes (Keypads do not display alarm activity from this point.)

When using Modem IIIa2 communication type, the unique point text should be set to “Hold-Up”, or equivalent language per the AHJ.

When using ContactID communication type, because the ContactID system doesn’t provide custom text, the hold-up point should be associated as a “hold-up” point at the receiving station. Set Area # Delay Restorals as follows:

- Area # Delay Restorals = No (Restoral report is sent when point restores.)

## 2.4 Guide to Programming Descriptions

Full configuration of the control panel is only achieved through use of the Remote Programming Software (RPS). A limited set of Tools are available via the keypad to modify some of the more commonly changed parameters.

This guide is set up in a specific order. Related program entries are grouped together in modules as they appear in RPS.

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

- The Program Item Prompt. Each prompt is shown as it appears in RPS. Refer to the *RPS Installation Guide* (P/N: 4998141259).
- 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.

## 2.5 Guide to Keypad Tools

GV4 now offers a series of tools for configuration and diagnostics through the use of the keypad with the Service Passcode only. The five configuration tools are:

- Programming. For a list of program items you can set using keypad Programming, refer to *Section 2.5.1 Keypad Programming Menu, page 12*. To access the Programming menu, the Keypad Programming option must be set to P (refer to *Section 3.12.5 Configuration Authority, page 101*), and all control panel areas must be disarmed.
- Service Bypass. For instructions to bypass a point using the keypad’s Service Bypass menu, refer to *Section 2.5.2 Service Bypass Menu, page 14*.
- RF Points. For a list of program items you can set using the keypad’s RF Points menu, refer to *Section 2.5.3 RF Points Menu, page 14*.
- RF Repeaters. For a list of program items you can set using the keypad’s RF Repeaters menu, refer to *Section 2.5.4 RF Repeaters Menu, page 15*.
- RF Diagnostics. For a list of diagnostic items you can perform using the keypad’s RF Diagnostics menu, refer to *Section 2.5.5 RF Diagnostics Menu, page 15*.
- IP Diagnostics. For a list of diagnostic items you can perform using the keypad’s IP Diagnostics menu, refer to *Section 8.3.1 IP Diagnostics Keypad Menu (B420), page 189*.

### 2.5.1 Keypad Programming Menu

| D1255 Keypad Programming Menu | | | | |
|---|---|---|---|---|
| 99 [ENT] →[NEXT] or [PREV] →TOOLS MENU [ENT] →ENTER PASSCODE (Installer) [ENT]→→→→→→→<br>→PROGRAMMING→ ↓ | | | | →→→<br>**Refer to Page** |
| **NOTICE!**<br>To move through the PROGRAMMING menu and submenus, press [NEXT] or [PREV].<br><br>To open a menu or submenu, press [ENT].<br><br>To exit to the previous level, press [ESC].<br><br>To send saved changes to the control panel, exit from PROGRAMMING mode. | →PHONE NUMBERS [ENT]→ | PHONE 1 - 4 | | *17* |
| | →PHONE PARAMETERS [ENT]→ | PHONE 1 - 4 | | *19* |
| | →ENHANCED COMM [ENT]→ | ↓ | | *40* |
| | | →COMMUNICATIONS | | *40* |
| | | →PATH 1 - 4 | | *40* |
| | →IP MODULE CONFIG [ENT]→ | B420 MODULE (1-2)↓ | | |
| | | →MODULE PARAM→ | ↓ | |
| | | | →DHCP ENABLE | *180* |
| | | | →UPnP ENABLE | *184* |
| | | →ADDRESS PARAM→ | ↓ | |
| | | | →IP ADDRESS | *180* |
| | | | →SUBNET MASK | *181* |
| | | | →DEFAULT GATEWAY | *182* |
| | | | →PORT NUMBER | *184* |
| | | →DNS PARAM→ | ↓ | |
| | | | →SERVER ADDRESS | *183* |
| | | | →MODULE HOSTNAME | *186* |
| | | →ENCRYPTION→ | ↓ | |
| | | | →AES KEY SIZE | *185* |
| | | | →AES KEY | *185* |
| | →ROUTING [ENT]→ | ROUTING GRP 1 - 4 | | *30* |
| | →RPS PARAMETERS [ENT]→ | ↓ | | |
| | | →RPS PASSCODE | | *55* |
| | | →RPS PHONE NUMBER | | *58* |
| | | →RPS IP ADDRESS | | *41* |
| | | →RPS IP PORT | | *48* |
| | →AREA PARAMETERS [ENT]→ | AREA NUMBER 1-32<br>(1 - 8 for D7412GV4)(1 - 4 for D7212GV4) | | *61* |
| | →COMMAND CENTER [ENT]→ | CC NUM 1 - 16 | | *80* and *81* |
| | →USER PASSCODE [ENT] | | | *126* |
| | →POINT PARAMETERS [ENT]→ | PT NUM 1-247<br>(1-75 for D7412GV4)(1-40 for D7212GV4) | | *146* |
| | →DISABLE KP PROG [ENT] | | | *101* |

| D1260 Keypad Programming Menu | | |
|---|---|---|
| 99 [ENTER] →[Next] →Tools Menu [ENTER] →ENTER PASSCODE (Installer) [ENTER]→→→→→→<br>→Programming→ ↓ | | →→→<br>**Refer to Page** |
| **NOTICE!**<br>To move through the Programming menu and submenus, press the **Next** softkey.<br><br>To open a menu or submenu, press [ENTER].<br><br>To exit to the previous level, press the **Exit** softkey.<br><br>To send saved changes to the control panel, exit from Programming mode. | →Phone Numbers [ENTER]→ Phone 1-4........ | *17* |
| | →Phone Parameters [ENTER]→ Phone 1-4........ | *19* |
| | →Enhanced Comm [ENTER]→ ↓ | *40* |
| | →Communications........ | *40* |
| | →Select IP Path→Path 1-4........ | *40* |
| | →IP Module Config [ENTER]→ B420 Module (1-2)↓ | |
| | →Module Parameters→ ↓ | |
| | →DHCP Enable.. | *180* |
| | →UPnP Enable.. | *184* |
| | →Address Parameters→ ↓ | |
| | →IP ADDRESS... | *180* |
| | →Subnet Mask.. | *181* |
| | →Default Gateway............ | *182* |
| | →Port Number.. | *184* |
| | →DNS Parameters→ ↓ | |
| | →Server Address............. | *183* |
| | →Module Hostname......... | *186* |
| | →Encryption→ ↓ | |
| | →AES Key Size.. | *185* |
| | →AES Encryption Key... | *185* |
| | →Routing [ENTER]→ Route Group 1-4........ | *30* |
| | →RPS Parameters [ENTER]→ ↓ | |
| | →RPS Passcode........ | *55* |
| | →RPS Phone Number........ | *58* |
| | →RPS IP Address........ | *41* |
| | →RPS IP Port........ | *48* |
| | →Area Parameters [ENTER]→ Area Number 1-32........<br>(1 - 8 for D7412GV4)(1 - 4 for D7212GV4) | *61* |
| | →Command Center [ENTER]→ CC Number 1-16........ | *80* and *81* |
| | →User Passcode [ENTER]........ | *126* |
| | →Point Parameters [ENTER]→ PT NUM 1-247........<br>(1-75 for D7412GV4)(1-40 for D7212GV4) | *146* |
| | →Disable Keypad Programming [ENT]........ | *101* |

### 2.5.2 Service Bypass Menu

| D1255 Service Bypass Menu | |
|---|---|
| 99 [ENT] →[NEXT] or [PREV] →TOOLS MENU [ENT] →ENTER PASSCODE (Installer) [ENT]→→→→→→→→→→<br>→SERVICE BYPASS [ENT]→ (Refer to Page *204*.) | |
| **NOTICE!**<br>Press [NEXT] to move through the list of bypassed points (when points are bypassed).<br>Press [ESC] to exit to the previous level. | |

| D1260 Service Bypass Menu | |
|---|---|
| 99 [ENTER] →[Next] →Tools Menu [ENTER] →Enter Passcode (Installer) [ENTER]→→→→→→→→→→→→→<br>→Service Bypass [ENTER]→ (Refer to Page *204*.) | |
| **NOTICE!**<br>Press the **Next** softkey to move through the list of bypassed points (when points are bypassed).<br>Press [Exit] to exit to the previous level. | |

### 2.5.3 RF Points Menu

| D1255 RF Points Menu | |
|---|---|
| 99 [ENT] →[NEXT] or [PREV] →TOOLS MENU [ENT] →ENTER PASSCODE (Installer) [ENT]→→→ | →→→→→→ |
| →RF POINTS [ENT]→ ↓ | **Refer to Page** |
| →ENROLL RF POINT [ENT]........................................................................ | *205* |
| →REPLACE RF POINT [ENT]...................................................................... | *205* |
| →REMOVE RF POINTS [ENT]..................................................................... | *206* |
| **NOTICE!**<br>Press [NEXT] or [PREV] to move through the RF POINTS menu and submenus.<br>Press [ENT] to open a menu or submenu.<br>Press [ESC] to exit to the previous level. | |

| D1260 RF Points Menu | |
|---|---|
| 99 [ENTER] →[Next] →Tools Menu [ENTER] →ENTER PASSCODE (Installer) [ENTER]→→→→→ | →→→→→→ |
| →RF Points [ENTER]→ ↓ | **Refer to Page** |
| →Enroll RF Point [ENT]........................................................................ | *205* |
| →Replace RF Point [ENT]...................................................................... | *205* |
| →Remove RF Points [ENT]..................................................................... | *206* |
| **NOTICE!**<br>Press the **Next** softkey to move through the RF Points menu and submenus.<br>Press [ENTER] to open a menu or submenu.<br>Press the **Exit** softkey to exit to the previous level. | |

### 2.5.4 RF Repeaters Menu

| **D1255 RF Repeaters Menu** | |
|---|---|
| 99 [ENT] →[NEXT] or [PREV] →TOOLS MENU [ENT] →ENTER PASSCODE (Installer) [ENT]→→→ | →→→→→→ |
| →RF REPEATERS [ENT]→ ↓ | **Refer to Page** |
| →ADD REPEATER [ENT]......................................................................... | *191* |
| →REPLACE REPEATER [ENT]................................................................ | *192* |
| →REMOVE REPEATER [ENT].................................................................. | *192* |
| **NOTICE!**<br>Press [NEXT] or [PREV] to move through the RF REPEATERS menu and submenus.<br>Press [ENT] to open a menu or submenu.<br>Press [ESC] to exit to the previous level. | |

| **D1260 RF Repeaters Menu** | |
|---|---|
| 99 [ENTER] →[Next] →Tools Menu [ENTER] →Enter Passcode (Installer) [ENTER]→→→→→ | →→→→→→ |
| →RF Repeaters [ENTER]→ ↓ | **Refer to Page** |
| →Add Repeater [ENTER]........................................................................ | *191* |
| →Replace Repeater [ENTER]................................................................ | *192* |
| →Remove Repeater [ENTER]................................................................. | *192* |
| **NOTICE!**<br>Press **Next** softkey to move through the RF Repeaters menu and submenus.<br>Press [ENTER] to open a menu or submenu.<br>Press the **Exit** softkey to exit to the previous level. | |

### 2.5.5 RF Diagnostics Menu

| **D1255 RF Diagnostics Menu** | | |
|---|---|---|
| 99 [ENT] →[NEXT] or [PREV] →TOOLS MENU [ENT] →ENTER PASSCODE (Installer) [ENT]→→→ | | →→→→→→ |
| → RF DIAGNOSTICS [ENT]→ ↓ | | **Refer to Page** |
| →RF POINTS [ENT]———————→ | ↓ | |
| | →STATES ....................... | *193* |
| | →SIGNAL STRENGTH..... | *193* |
| RF REPEATER .......................................................................................... | | |
| **NOTICE!**<br>Press [NEXT] or [PREV] to move through the RF DIAGNOSTICS menu and submenus.<br>Press [ENT] to open a menu or submenu.<br>Press [ESC] to exit to the previous level. | | |

| **D1260 RF Diagnostics Menu** | | |
|---|---|---|
| 99 [ENTER]→ [Next] →Tools Menu [ENTER] →Enter Passcode (Installer) [ENTER]→→→→→ | | →→→→→→ |
| → RF Diagnostics [ENTER]→ ↓ | | **Refer to Page** |
| →RF Points [ENTER]———————→ | ↓ | |
| | →States ........................ | *193* |
| | →Signal Strength........... | *193* |
| RF Repeater ............................................................................................ | | |
| **NOTICE!**<br>Press **Next** softkey to move through the RF Diagnostics menu and submenus.<br>Press [ENTER] to open a menu or submenu.<br>Press the **Exit** softkey to exit to the previous level. | | |

## 2.5.6 IP Diagnostics Menu

| **D1255 IP Diagnostics Menu** | |
|---|---|
| 99 [ENTER]→ [Next]→ Tools Menu [ENTER]→ ENTER PASSCODE (Installer) [ENTER]→→→→→→→→ | →→→ |
| → IP DIAGNOSTICS [ENT]→ B420 MODULE (1-2) ↓ | **Refer to Page** |
| →SETTINGS [ENT]................................................... | *189* |
| →CONNECTION TEST [ENT].................................... | *189* |
| **NOTICE!**<br>Press [NEXT] or [PREV] to move through the IP DIAGNOSTICS menu and submenus.<br>Press [ENT] to open a menu or submenu.<br>Press [ESC] to exit to the previous level. | |

| **D1260 IP Diagnostics Menu** | |
|---|---|
| 99 [ENTER]→ [Next]→ Tools Menu [ENTER]→ Enter Passcode (Installer) [ENTER]→→→→→→→→→ | →→→ |
| → IP Diagnostics [ENT]→ B420 Module (1-2) ↓ | **Refer to Page** |
| →Settings [ENT]......................................................... | *189* |
| →Connection Test [ENT]................................................. | *189* |
| **NOTICE!**<br>Press **Next** softkey to move through the IP Diagnostics menu and submenus.<br>Press [ENTER] to open a menu or submenu.<br>Press the **Exit** softkey to exit to the previous level. | |

# 3 Panel and Area Wide Parameters

This section has fourteen programming categories.

- Phone
- Phone Parameters
- Routing
- Enhanced Communications
- SDI Enhanced Communications
- Power Supervision
- Printer parameters
- RPS Parameters
- Miscellaneous
- Area Parameters
- Keypad
- User Interface
- Function List
- Relay Parameters

## 3.1 Phone

The control panel can dial as many as four different telephone numbers when sending event reports. Refer to *Section 3.3 Routing, page 23* for information about event report routing and communication protocols.

ⓘ **NOTICE!**
When using PSTN telephone lines, program two telephone numbers to meet UL 864 requirements (D9412GV4 and D7412GV4).

**Phone #**

| | |
|---|---|
| **Default:** | Blank |
| **Selection:** | Up to 24 characters |
| 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.<br>Programming this item Blank does not disable phone routing. To disable reporting to this phone, refer to *Section 3.3 Routing, page 23*. |

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 3.3 Routing, page 23*.

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

ModemIIIa$^2$ 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 #** table to define dialing characteristics.

**For SIA CP-01 Compliance**

**Call Waiting Disable**

If the telephone system at the installation site uses the Call Waiting feature, ensure that the primary 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.

⚠ **CAUTION!**

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

ⓘ **NOTICE!**

Example: If the central station telephone number is 555-1234, and the primary Route Group destination is Phone 1, program Phone 2 with the following sequence: *70C5551234.

**Keypad Programming of Phone #**

**D1255**

1. Refer to *Section 3.2 Phone Parameters, page 19* to access Programming and navigate to the **PHONE NUMBERS** option.
2. At the **PHONE 1 - 4** prompt, enter the phone number you wish to configure and press [ENT]. The current phone number shows.

ⓘ **NOTICE!**

If the current phone number is longer than 20 characters, use the [PREV] and [NEXT] keys to scroll to view the additional characters.

3. Press [ENT] to change the phone number.
4. The [PREV] button acts as a [Backspace] key and the [COMMAND] key scrolls through special characters. Press [PREV] to delete the characters of the phone number, and then enter the new phone number. Press [COMMAND] to cycle through the special dialing characters {*, #, C, D}, then press [NEXT] to choose a character.
5. Press [ENT] to save the phone number.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 3.2 Phone Parameters, page 19* to access Keypad Programming and navigate to the **Phone Numbers** option and press the corresponding softkey.
2. At the **Phone (1-4)** prompt, enter the phone number you wish to configure and press [ENTER]. The current phone number shows.

ⓘ **NOTICE!**

If the current phone number is longer than 20 characters, the **Previous** and **Next** softkeys appear. Use the softkeys to scroll to view the additional characters.

3. Press the **Edit** softkey to change the phone number.

4. The **Pause** (3-sec pause - "C") and **DT Detect** (Dial Tone Detect - "D") softkeys enter special characters. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire phone number. The [COMMAND] and [ENTER] keys allow you to enter an * or a #. Use the softkeys, the number buttons, and the [COMMAND] and [ENTER] keys on the keypad to enter the new phone number.
5. Press the **Save** softkey.

When the keypad reads **Parameter Saved**, your selection has been configured.

## 3.2 Phone Parameters

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

### Phone # Format

| | |
|---|---|
| **Default:** | ModemIIIa$^2$ |
| **Selection:** | ModemIIIa$^2$ or Contact ID |
| ModemIIIa$^2$ | ModemIIIa$^2$ Communication Format |
| Contact ID | 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.

Reports identify points as 001 through 247 and passcode User ID codes as 000 through 999 at the D6500 or D6600 Receiver (unless Point/User Flag is programmed Yes; refer to *Section Point/User Flag, page 19* in this section). When reporting point events, ModemIIIa$^2$ Communication Format also sends point text to the D6500 or D6600 as programmed in Point Assignments.

### Keypad Programming of Phone # Format

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **PHONE PARAMETERS** option.
2. At the **PHONE 1 - 4** prompt, enter the phone route number you wish to configure and press [ENT].
3. Press [NEXT] or [PREV] to toggle between Contact ID and ModemIIIa$^2$ and press [ENT] to select the desired phone format.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1265**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Phone Parameters** option and press the corresponding softkey.
2. At the **Phone (1 - 4)** prompt, enter the phone route number you wish to configure and press [ENTER]. The current configuration shows.
3. Press the **Edit** softkey to change the phone format.
4. Select the softkey for the option you wish to change. Press the **Save** softkey.

When the keypad reads **Parameter Saved**, your selection has been configured.

### Point/User Flag

| | |
|---|---|
| **Default:** | No |
| **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 *Table 3.1, Page 20* and *Table 3.2, Page 21* 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 Appendix C in the *Conettix D6600/D6100 Receiver/Gateway Computer Interface Manual* (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 999 (rather than 000 to F08), as indicated in *Table 3.1, Page 20* and *Table 3.2, Page 21*. |

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 **Phone # Format** is **ModemIIIa$^2$**, the control panel sends expanded Bosch ModemIIIa$^2$ 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 **Phone # Format** is **ModemIIIa$^2$**, the control panel sends expanded Bosch ModemIIIa$^2$ Communication Format Reports to the receiver. **Point/User Flag** affects Bosch ModemIIIa$^2$ Communication Format data as shown in *Table 3.1, Page 20*. The Bosch Security Systems, Inc. D6500 or D6600 Receiver adds the leading zero in the User ID number with **Point/User Flag** programmed **No**.

| **Point/User Flag No** | **Point/User Flag Yes** |
|---|---|
| 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 999 | 000 |

**Table 3.1** ModemIIIa2 Communication Format Data - User ID 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 to 247 | 717 to 731 |

**Table 3.2** ModemIIIa2 Communication Format Data - Point Numbers

### 3.2.1 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 (*Section 4.1 Passcode or Token Worksheet, page 125*). 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 3.3, Page 21*.

| 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 | | |

**Table 3.3** D6000 User IDs and Zones

**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 Supervision Time

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 10 to 240 |
| 0 | 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.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), 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. |

**NOTICE!**
To meet UL 864 requirements, set this parameter to No.
Phone Supervision 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:** | Yes |
| **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. |

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), set this parameter to **Yes**.

**NOTICE!**
Phone Supervision 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. |

**NOTICE!**
When using two telephone lines, set this parameter to Yes to meet UL 864 requirements (D9412GV4 and D7412GV4).

**NOTICE!**
Program Phone Supervision Time when using two phone lines.

**NOTICE!**
The D7212GV4 does not support the use of the D928 Dual Phone Line Switcher. Leave this prompt set to its default value.

**Expand Test Report**

| | |
|---|---|
| **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 6 Schedules (Skeds), page 154*.

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

## 3.3 Routing

Use routing to select full or partial groups of events to report to up to eight different destinations (four over phone, four over network). 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.
Event routing can be sent 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 or B420. Sending events over GPRS requires a special (ITS-DX4020-G).

### 3.3.1 Call 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. GV4 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.

### 3.3.2 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.

### 3.3.3 Programming Primary and Backup Destinations

Each route number has an **R# Primary Device** and an **R# Backup Device**. For example, if 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 Network Interface Module.

With enhanced communications, the **R# Primary Device** destination can be either the phone number or an SDI route path 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# BackupDevice** destination.

### 3.3.4 Enhanced Routing

The GV4 Series Control Panels allow events to be sent to up to four network destinations. The network interface modules (s) connect directly to the SDI or SDI2 Bus and occupy SDI Addresses 88 or 92 or SDI2 Addresses 1 or 2. For additional information regarding the specific programming requirements for enhanced communications, refer to *Section 3.4 Programming Path Numbers and Network Addresses for Enhanced Communications, page 40*.

An enhanced communication route is a combination of a path network destination and a communication device, so there are up to 16 possible enhanced communication routes available.

A single network interface module (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** (Refer to *Section 3.3 Routing, page 23*.)

1. Select Route Group 1
2. Program a **SDI 88 Path 1** for **RG1 Primary Destination**

3. Program a **Phone 1** for **RG1 Backup Destination**
4. Enable all applicable events to be included in Route Group 1.

- **Phone** (Refer to *Section 3.1 Phone, page 17*.)

1. Select Phone 1.
2. Program Phone 1 with the applicable central station receiver phone number.

- **Enhanced Communication** (Refer to *Section 3.4 Programming Path Numbers and Network Addresses for Enhanced Communications, page 40*).

1. Set **Enhanced Comm** to **Yes**.
2. Program **Path 1 Nework Address** with the applicable central station network address.
3. Program **Path 1 Port Num** with the applicable central station network receiver port number.
4. Enter a non-zero value for the **Path 1 Poll Rate**.

### 3.3.5 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.

### 3.3.6 Routing Destination Communication Failures

When the **R# Primary Device** fails to connect to the central station receiver after two attempts by phone, 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. 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 3.4, Page 25*.

| Device | Path 1 | Path 2 | Path 3 | Path 4 |
|---|---|---|---|---|
| SDI 88 | 88 | 89 | 90 | 91 |
| SDI 92 | 92 | 93 | 94 | 95 |
| SDI2-1 | 11 | 21 | 31 | 41 |
| SDI2-2 | 12 | 22 | 32 | 42 |

**Table 3.4** SDI Path Number by Device

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 network) or a successful poll (via network) 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 *Section Path # Poll Rate, page 41*.

### 3.3.7 Message Prioritization within a Route Number

The GV4 Series 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.

**NOTICE!**

To comply with NFPA and UL 864 (D9412GV4 and D7412GV4), program **Route 1** to send a report of only Fire Alarm Events to ensure the fastest reporting time.

### Event Priority

*Table 3.5, Page 29* shows the description of each event, its priority, and Modem IIIa$^2$ Event Code.

| Event Description | Event Priority | Modem IIIa$^2$ Event Code |
|---|---|---|
| Fire Alarm | 1 | 11 |
| Fire Alarm Restoral | 5 | 14 |
| Fire Missing | 5 | 13 |
| Fire Trouble | 5 | 12 |
| Fire Supervision | 5 | 124 |
| Fire Restoral (after Tbl, Msg, Bypass) | 5 | 15 |
| Fire Cancel | 4 | 27 |
| Fire Supervision Missing | 5 | 146 |
| Fire Supervision Restore | 5 | 123 |
| Alarm Report | 3 | 16 |
| Duress | 2 | 4 |
| Missing Alarm | 6 | 19 |
| User Code Tamper | 8 | 55 |
| Trouble Report | 6 | 17 |
| Missing Trouble | 8 | 20 |
| Non-Fire Supervision | 6 | 78 |
| Point Bus Fail | 6 | 24 |
| Point Bus Restoral | 6 | 91 |
| Non-Fire Cancel | 4 | 45 |
| Alarm Restore | 6 | 26 |
| Supervision Missing | 8 | 147 |
| Unverified Event | 6 | 169 |
| Point Bypass/Command Bypass | 7 | 7 |
| Forced Point | 7 | 8 |
| Point Opening | 8 | 21 |
| Point Closing | 8 | 22 |
| Was Force Armed | 7 | 34 |
| Fail To Open | 8 | 40 |
| Fail To Close | 8 | 41 |
| Extend Close Time | 8 | 44 |
| Opening Report | 8 | 47 |
| Forced Close | 7 | 48 |
| Closing Report | 8 | 50 |
| Forced Close Perimeter Instant | 7 | 84 |
| Forced Close Perimeter Delay | 7 | 85 |
| Perimeter Instant Armed | 8 | 88 |
| Perimeter Delay Armed | 8 | 89 |
| 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 | 8 | 35 |
| S: Open | n/a | n/a |
| S: Close | n/a | n/a |
| Test Report | 8 | 51 |
| 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 |

| **Event Description** | **Event Priority** | **Modem IIIa$^2$ Event Code** |
|---|---|---|
| S: Door Left Open | n/a | n/a |
| SDI Device Failure* | 4 | 70 |
| SDI Device Restoral* | 8 | 71 |
| Watchdog Reset | 4 | 77 |
| Parameter Checksum Fail | n/a | n/a |
| Reboot | 8 | 82 |
| Phone Line Fail | 4 | 68 |
| Phone Line Restoral | 8 | 69 |
| AC Failure | 4 | 72 |
| AC Restoral | 8 | 73 |
| Battery Missing | 4 | 74 |
| Battery Low | 4 | 75 |
| Battery Restoral | 8 | 76 |
| Route Comm Fail | 4 | 66 |
| Route Comm Restore | 8 | 67 |
| Checksum Fail | n/a | n/a |
| Sensor Reset | 7 | 31 |
| Relay Set | 7 | 32 |
| Relay Reset | 7 | 33 |
| Sked Executed | 7 | 57 |
| Sked Changed | 7 | 58 |
| Fail to Execute | 8 | 151 |
| Event Log Threshold | 8 | 52 |
| Event Log Overflow | 8 | 53 |
| Parameters Changed | 8 | 54 |
| RPS Access OK | 8 | 64 |
| RPS Access Fail | 8 | 65 |
| Remote Reset | 8 | 79 |
| Program Access OK | n/a | n/a |
| Program Access Fail | n/a | n/a |
| Service Start | 8 | 29 |
| Service End | 8 | 30 |
| Fire Walk Start | 8 | 36 |
| Fire Walk End | 8 | 37 |
| Walk Test Start | 8 | 38 |
| Walk Test End | 8 | 39 |
| Extra Point | 8 | 23 |
| Send Point Text | n/a | n/a |
| RF Low Battery | 6 | 93 |
| RF Battery Restore | 6 | 94 |
| Date Changed | 8 | 59 |
| Time Changed | 8 | 60 |
| Delete User | 8 | 90 |
| User Code Change | 8 | 56 |
| Area Watch | 8 | 42 |
| Card Assigned | 8 | 110 |
| Change Level | 7 | 61 |
| Access Granted | 8 | 3 |
| No Entry | 8 | 115 |
| Door Left Open | 8 | 116 |
| Cycle Door | 8 | 112 |
| Door Unlocked | 8 | 113 |
| Door Secure | 8 | 114 |
| Door Request | 8 | 117 |
| Door Locked | 8 | 145 |

| Event Description | Event Priority | Modem IIIa[2] Event Code |
|---|---|---|
| User Alarm COMMAND 7 | 2 | 5 |
| User Alarm COMMAND 9 | 2 | 6 |
| Card Assigned[1] | 8 | 110 |
| Change Level[1] | 7 | 61 |
| Access Granted[1] | 8 | 3 |
| No Entry1 | 8 | 115 |
| Door Left Open[1] | 8 | 116 |
| Cycle Door[1] | 8 | 112 |
| Door Unlocked[1] | 8 | 113 |
| Cycle Door[1] | 8 | 112 |
| Door Unlocked[1] | 8 | 113 |
| Door Secure[1] | 8 | 114 |
| Door Request[1] | 8 | 117 |
| Door Locked[1] | 8 | 145 |
| User Alarm COMMAND 7 | 2 | 5 |
| User Alarm COMMAND 9 | 2 | 6 |
| RF Interference | 8 | 103 |
| RF Interference Restoration | 8 | 135 |
| Equipment Fail | 8 | 70 |
| Equipment Fail Restoration | 8 | 71 |
| Service Bypass | 7 | 139 |
| Service Bypass Restoration | 7 | 140 |
| [1] This event is not transmitted for the D7212GV4. Use only the default setting. | | |

**Table 3.5** Event Priority

### 3.3.8 Route Group Parameters

The **RG # Same Network Receiver** parameters define whether a primary and backup network receiver configured within a Route Group are the same receiver. This is required to ensure that the authentication keys from the control panel to receiver are the same when the paths to the receiver use different IP Addresses or Port Numbers. These parameters also enable the backup path poll time to change to the primary poll time in the event of a Communication Trouble condition. This operates 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 receiver that can be accessed from more than one network such as on a LAN/WAN and over the Internet (even if they have different IP/port settings).
- Either the primary or the backup path (not both) has a Communication Trouble condition.

**RG# Same Network Receiver**

| | |
|---|---|
| **Default** | Yes |
| **Selection:** | Yes or No |
| Yes | The control panel uses the same authentication keys to communicate with both the primary and backup paths that are the same receiver and 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 | The control panel uses separate authentication keys to communicate with the primary and backup receivers and upon detection of a Communication Trouble on either the primary or backup enhanced communication paths, the working path continues to use its configured poll rate. |

**For Example:** This would be used when a DX4020 is reporting to a receiver over a LAN/ WAN and a ITS-DX4020-G is reporting to the same receiver over the Internet from the cellular service provider. This configuration also typically has the poll rate for the ITS-DX4020-G set to a slower poll rate than the primary such as every 4 hours.

**NOTICE!**

In the above example, if there is a Communication Trouble Condition on the DX4020, then the ITS-DX4020-G will poll at the configured poll rate of the DX4020. If the poll rate of the DX4020 is set to 5 minutes or faster, there is a possibility of excessive data usage that may exceed your data plan with the cellular service provider. Be sure that any Communication Trouble events are addressed as soon as possible.

## 3.3.9 Communication Attempts

The control panel makes up to ten communication attempts using the primary and backup devices within a route group. If unsuccessful, it sends a Comm Fail Report. The communication 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.

There are four Route Groups which contain a selection of event categorizes and individual events. 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:** | No Device |
| **Selection:** | No Device, Phone 1..4, SDI ## Path 1..4 |
| Phone 1 | Phone 1 is this group’s primary destination. |

| | |
|---|---|
| Phone 2 | Phone 2 is this group’s primary destination. |
| Phone 3 | Phone 3 is this group’s primary destination. |
| Phone 4 | Phone 4 is this group’s primary destination. |
| SDI 88 Path 1 | Path 1 on SDI 88 is this group's primary destination. |
| SDI 88 Path 2 | Path 2 on SDI 88 is this group's primary destination. |
| SDI 88 Path 3 | Path 3 on SDI 88 is this group's primary destination. |
| SDI 88 Path 4 | Path 4 on SDI 88 is this group's primary destination. |
| SDI 92 Path 1 | Path 1 on SDI 92 is this group's primary destination. |
| SDI 92 Path 2 | Path 2 on SDI 92 is this group's primary destination. |
| SDI 92 Path 3 | Path 3 on SDI 92 is this group's primary destination. |
| SDI 92 Path 4 | Path 4 on SDI 92 is this group's primary destination. |
| SDI2-1 Path 1 | Path 1 on SDI2-1 is this group's primary destination. |
| SDI2-1 Path 2 | Path 2 on SDI2-1 is this group's primary destination. |
| SDI2-1 Path 3 | Path 3 on SDI2-1 is this group's primary destination. |
| SDI2-1 Path 4 | Path 4 on SDI2-1 is this group's primary destination. |
| SDI2-2 Path 1 | Path 1 on SDI2-2 is this group's primary destination. |
| SDI2-2 Path 2 | Path 2 on SDI2-2 is this group's primary destination. |
| SDI2-2 Path 3 | Path 3 on SDI2-2 is this group's primary destination. |
| SDI2-2 Path 4 | Path 4 on SDI2-2 is this group's primary destination. |

**NOTICE!**
To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), program a **Primary Device**.

Select the communication device and the primary destination.
Refer to *Section 3.4 Programming Path Numbers and Network Addresses for Enhanced Communications, page 40* to enable enhanced communication paths.

**Keypad Programming of R# Primary Device**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **ROUTE GRP 1 - 4** option.
2. At the **ROUTE GRP 1 - 4** prompt, enter the route group number you wish to configure and press [ENT]. The keypad reads **RT GRP 1 PRIMARY**, and then the current configuration (for example, SDI 88 PATH 4).
3. To change the configuration, press [ENT] when the current configuration shows, and then press [NEXT] or [PREV] to scroll through the options, as listed in *Section  R# Primary Device, page 30*.
4. When the keypad reads the desired configuration option, press [ENT] to select it.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Route Group 1 - 4** option.
2. At the **Route Group 1 - 4** prompt, enter the route group number you wish to configure and press [ENTER]. The keypad reads **Rt Group 1 Primary**, and then the current configuration (for example, SDI 88 PATH 4).
3. To change the configuration, press the **Edit** softkey, and then press the **Next** or the **Previous** softkey to scroll through the options, as listed in *Section  R# Primary Device, page 30*.
4. When the keypad reads the desired configuration option, press the **Save** softkey to select it.

When the keypad reads **Parameter Saved**, your selection has been configured.

**R# Backup Device**

| | |
|---|---|
| **Default:** | No Device |
| **Selection:** | No Device, Phone 1..4, SDI ## Path 1..4 |
| Phone 1 | Phone 1 is this group’s backup destination if the primary destination fails. |
| Phone 2 | Phone 2 is this group’s backup destination if the primary destination fails. |
| Phone 3 | Phone 3 is this group’s backup destination if the primary destination fails. |
| Phone 4 | Phone 4 is this group’s backup destination if the primary destination fails. |
| SDI 88 Path 1 | Path 1 on SDI 88 is this group's backup destination if the primary destination fails. |
| SDI 88 Path 2 | Path 2 on SDI 88 is this group's backup destination if the primary destination fails. |
| SDI 88 Path 3 | Path 3 on SDI 88 is this group's backup destination if the primary destination fails. |
| SDI 88 Path 4 | Path 4 on SDI 88 is this group's backup destination if the primary destination fails. |
| SDI 92 Path 1 | Path 1 on SDI 92 is this group's backup destination if the primary destination fails. |
| SDI 92 Path 2 | Path 2 on SDI 92 is this group's backup destination if the primary destination fails. |
| SDI 92 Path 3 | Path 3 on SDI 92 is this group's backup destination if the primary destination fails. |
| SDI 92 Path 4 | Path 4 on SDI 92 is this group's backup destination if the primary destination fails. |
| SDI2-1 Path 1 | Path 1 on SDI2-1 is this group's backup destination if the primary destination fails. |
| SDI2-1 Path 2 | Path 2 on SDI2-1is this group's backup destination if the primary destination fails. |
| SDI2-1 Path 3 | Path 3 on SDI2-1 is this group's backup destination if the primary destination fails. |
| SDI2-1 Path 4 | Path 4 on SDI2-1 is this group's backup destination if the primary destination fails. |
| SDI2-2 Path 1 | Path 1 on SDI2-2 is this group's backup destination if the primary destination fails. |
| SDI2-2 Path 2 | Path 2 on SDI2-2 is this group's backup destination if the primary destination fails. |
| SDI2-2 Path 3 | Path 3 on SDI2-2 is this group's backup destination if the primary destination fails. |
| SDI2-2 Path 4 | Path 4 on SDI2-2 is this group's backup destination if the primary destination fails. |

**NOTICE!**

To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), program a **Backup Device**.

Select the communication device and the backup destination. The backup device is used when the primary device fails to reach the programmed destination.

Refer to *Section 3.4 Programming Path Numbers and Network Addresses for Enhanced Communications, page 40* to enable enhanced communication paths.

**Keypad Programming of the R# Backup Device**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **ROUTE GRP 1 - 4** option.
2. At the **ROUTE GRP 1 - 4** prompt, enter the route group number you wish to configure and press [ENT]. The keypad reads **RT GRP 1 PRIMARY**, and then the current configuration (for example, SDI 88 PATH 4).
3. Press [NEXT] to advance to the **RT GRP 1 BACKUP** option. The Primary device cannot be set to **No Device** before setting the Backup Destination.
4. To change the configuration, press [ENT] when the current configuration shows, and then press [NEXT] or [PREV] to scroll through the options, as listed in *Section  R# Backup Device, page 32*.
5. When the keypad reads the desired configuration option, press [ENT] to select it.

When the keypad reads **Parameter Saved**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Route Group 1 - 4** option.
2. At the **Route Group 1 - 4** prompt, enter the route group number you wish to configure and press [ENTER]. The keypad reads **Rt Group 1 Primary**, and then the current configuration (for example, SDI 88 PATH 4).
3. Press the **Backup** softkey. The keypad reads **Rt Group 1 Primary**, and then the current configuration (for example, SDI 88 PATH 4). The Primary device cannot be set to **No Device** before setting the Backup Destination.
4. To change the configuration, press the **Edit** softkey, and then press the **Next** or the **Previous** softkey to scroll through the options, as listed in *Section  R# Backup Device, page 32*.
5. When the keypad reads the desired configuration option, press the **Save** softkey to select it.

When the keypad reads **Parameter Saved**, your selection has been configured.

## 3.3.10 Route Group Categories

**Fire Reports**

**NOTICE!**

To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), enable Fire Reports.

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

| Report | Selection | 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 Supervision | **Yes**, No | Fire supervisory |
| 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 |

**Table 3.6** Fire Reports

### Burglar Reports

Select **Yes** to send a report when the event occurs. Refer to *Table 3.7, Page 34*.

| Report | Selection | 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 Report | **Yes**, No | Trouble Event |
| R# Missing Trbl | **Yes**, No | Missing Trouble Event |
| R# Non Fire Suprv | **Yes**, No | Non-fire Supervisory 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 |

**Table 3.7** Burglar Reports

**NOTICE!**

**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.

**NOTICE!**

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

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

| Report | Selection | 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 ClosTm | **Yes**, No | Extend Close Time Event |
| R# Opening Report | Yes, **No** | Opening Events |
| R# Forced Close | Yes, **No** | Point Forced Close Event |
| R# Closing Report | Yes, **No** | Closing Events |
| R# FC Perimeter Inst | Yes, **No** | Forced Close Perimeter Instant Armed Event |
| R# FC Perimeter Delay | Yes, **No** | Forced Close Perimeter Delay Armed Event |
| R# Perimeter Inst Arm | Yes, **No** | Perimeter Instant Armed Event |
| R# Perimeter Delay Arm | Yes, **No** | Perimeter Delay Armed Event |
| R# Send User Text | **Yes**, No | User text |

**Table 3.8** User Reports

### Test Reports

**NOTICE!**
To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), 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 *Section Table 3.9 Test Reports, page 36*.

**Manual**: To send a single Test Report manually, enter [COMMAND][4][1] at the keypad. Refer to *Section Send Report, page 96*.

To expand this Test Report to include any off-normal point condition or other off-normal system conditions, Expand Test Report (*Section Expand Test Report, page 23*) must be programmed Yes. Refer to the footnotes with *Table 3.10, Page 37* 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 3.9, Page 36*, 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 3.9, Page 36*, enter [COMMAND][4][2] at the keypad. Refer to *Section View Memory, page 96*.

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.

| Report | Selection | 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: Perimeter Inst[1] | **Yes**, No | Status Perimeter Instant Arm |
| R# S: Perimeter 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 |
| [1]Information about this condition is sent with a Status Report.<br>[2] Information about this condition is sent as **S: Trouble Event** with a Status Report.<br>[3] Information about this condition is sent as **S: Alarm Event** with a Status Report. | | |

**Table 3.9** Test Reports

### Diagnostic 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 3.10, Page 37* still exists, the events report when a Test Report is enabled and **Expanded Test Report** is programmed **Yes**. Refer to the **Test Reports** sub-prompt in *Section 3.3.9 Communication Attempts, page 30*.

| Report | Selections | Report Description |
|---|---|---|
| R# SDI Device Fail[1] | **Yes**, No | SDI device failure |
| R# SDI Device Restoral | **Yes**, No | Restoral of SDI device failure |
| R# Watchdog Reset | **Yes**, No | Watchdog Reset Event |
| R# Parameter Checksum Fail | **Yes**, No | Parameter checksum failure |
| R# Reboot | **Yes**, No | Reboot Event |
| R# Phone Line Fail[1] | **Yes**, No | Failure of phone line |
| R# Phone Line Restoral | **Yes**, No | Restoral of phone line afterfailure |
| R# AC Fail[1], [2] | **Yes**, No | Failure of AC power to control panel |
| R# AC Restoral [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 Restoral [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 Restoral | **Yes**, No | Restoral of communication to specific route after a failure |
| R# Rt Comm Restoral | **Yes**, No | Restoral of communication to specific route after a failure |
| R# Checksum Fail | **Yes**, No | Checksum Fail Event |
| R# Network Fail[4] | Yes, **No** | Failure of network |
| R# Network Restoral[4] | Yes, **No** | Restoral of network |
| R# Network Condition[4] | Yes, **No** | Condition of network |
| R# RF Interference | **Yes**, No | RF receiver interference |
| R# RF Interference Restoration | **Yes**, No | RF receiver communication restored |
| R# Equipment Fail | **Yes**, No | Trouble on SDI2 device |
| R# Equipment Fail Restoration | **Yes**, No | Restoration of trouble on SDI2 device |

[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 (D9412GV4 and D7412GV4), 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.

**Table 3.10** Diagnostic Reports

**NOTICE!**

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.

| 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 |

ⓘ **NOTICE!**

When activating an on-board relay using remote automation software, the GV4 Series Control Panels log and print the resulting event as:

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

**Auto Function Reports**

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

| **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.

ⓘ **NOTICE!**

"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. "Fail to Call RPS" indicates that control panel called RPS, but was unable to connect.

| **Report** | **Selections** | **Report Description** |
|---|---|---|
| R# Log Threshold | **Yes**, No | Reports Service Walk Test Start Event |
| R# Service End | **Yes**, No | Service Walk Test End Event |
| R# Parameters Changed | **Yes**, No | RPS Parameters were changed |
| R# RPS Access OK | **Yes**, No | Successful RPS access |
| R# RPS Access Fail | **Yes**, No | RPS failed to access control panel |
| R# Remote Reset | **Yes**, No | Control panel reset by RPS |
| R# Program Access OK | **Yes**, No | Successful local programming |
| R# Program Access Fail | **Yes**, No | Local programming failed |

**Table 3.11** RPS Reports

**Point Reports**

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

| **Report** | **Selections** | **Report Description** |
|---|---|---|
| R# Service Start | **Yes**, No | Reports Service Walk Test Start Event |
| R# Service End | **Yes**, No | Service Walk Test End Event |
| R# Fire Walk Start | **Yes**, No | Fire Walk Start Event |
| R# Fire Walk End | **Yes**, No | Fire Walk End Event |
| R# Walk Test Start | **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[1] | **Yes**, No | Point Text |
| R# RF Low Battery | Yes, **No** | Low battery conditions for RF points |
| R# RF Low Battery Restore | Yes, **No** | Low battery restoral conditions for RF points |
| R# Service Bypass | Yes, **No** | Point was removed from service |
| R# Service Bypass Restoration | Yes, **No** | Yes/NoPoint was returned to service |
| [1] Point text is always transmitted when using network applications. | | |

**Table 3.12** Point Reports

### User Change Reports

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

| **Report** | **Selections** | **Report Description** |
|---|---|---|
| R# Date Changed | **Yes**, No | Reports Date Changed Event |
| R# Time Changed | **Yes**, No | Reports Time Changed Event |
| R# Delete User | **Yes**, No | Reports Deleted User, Token and Key fob Event |
| R# User Code Change | **Yes**, No | Reports User Passcode Added or Changed Event |
| R# Area Watch | **Yes**, No | Reports Area Watch Start and Watch End Event |
| R# Card/Key Fob Assigned | **Yes**, No | Reports Access Credential or Key fob Assigned to User Event |
| R# Key Fob Removed | **Yes**, No | Reports Key Fob Removed From System Event |
| R# Change Level | **Yes**, No | Reports User Authority Level Change Event |

**Table 3.13** User Change Reports

### Acces Reports

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

| **Report** | **Selections** | **Report Description** |
|---|---|---|
| Access Granted | **Yes**, No | Reports Access Denied Events |
| No Entry | **Yes**, No | Reports Door Left Open Event |
| Door Left Open | **Yes**, No | Reports Deleted User, Token and Key fob Event |
| Cycle Door | **Yes**, No | Reports Door Momentarily Unlocked Events (Unsupported) |
| Door Unlocked | **Yes**, No | Reports Door Held Open (Unlocked) Events |
| Door Secure | **Yes**, No | Reports Door Held Closed (Secured) Events |
| Door Request | **Yes**, No | Reports Request to Enter and Request to Exit Events |
| Door Locked | **Yes**, No | Reports Door Locked Events |

**Table 3.14** Access Reports

## 3.4 Programming Path Numbers and Network 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 3.3 Routing, page 23*.

**Enhanced Comm**

| | |
|---|---|
| **Default** | Yes |
| **Selection:** | Yes or No |
| Yes | Enable enhanced communications over the SDI or SDI2 bus. |
| No | Do not enable enhanced communications over the SDI or SDI2 bus. |

**NOTICE!**
If using a network as the communication means for UL 864 Commercial Fire applications (D9412GV4 and D7412GV4), set this parameter to **Yes**.

Determines if the control panel allows enhanced communications over the SDI bus.
Events can be routed to as many as four possible network destinations over communication modules on either the SDI or SDI2 bus. The communication device and path destination are called the route and are selected for each route group with the **RG# Primary Device** and **RG# Backup Device** prompts.
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 *Section  Path # Network Address, page 41*).
If events are to be routed to an SDI Path but not to an IP Address, allow the setting for **Path # Network Address** to remain at **0**. **Path # Poll Rate**, **Path # Ack Wait**, and **Path # Retry Count** must be programmed.

**Keypad Programming to Enable or Disable Enhanced Comm**
**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **ENHANCED COMM** option. Press [ENT].
2. The keypad shows the current setting by alternating between **COMMUNICATIONS>** and **ENHANCED> YES or NO**. To configure enhanced communications, press [ENT].
3. Press [NEXT] or [PREV] to toggle to **YES** to enable enhanced communication or **No** to disable enhanced communication, and then press [ENT].

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Enhanced Comm** option. Press the **Enhanced Comm** softkey.
2. The current Enhanced Enabled configuration shows (for example, Enhanced Enabled: Yes).
3. Press the **Edit** softkey to change the configuration.
4. Press the **Yes** or **No** softkey, and then press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

### Path # Network Address

| | |
|---|---|
| **Default** | Blank |
| **Selection:** | 0.0.0.0 to 255.255.255.255 or [host name] |
| 0 to 255 | There are four numbers for an IPV4 address. Leading zeros are not required. A host name can be used if a B420 network communication module is installed on the control panel. |

**NOTICE!**
If using a network as the communication means for UL 864 Commercial Fire applications (D9412GV4 and D7412GV4), set **Path # Network Address** as necessary.

**Path # Network Address** contains the network host name or the IPV4 address for each of the four enhanced communication paths available.
A network address has four fields. Each field has a range of 0 to 255. For example, an IPv4 address is expressed as 110.227.64.190. Contact your network administrator to obtain the appropriate IPv4 address or host name to contact a central station receiver. If a B420 Ethernet Communication Module is installed, then the control panel has the option to use a host name for the Path route Network Address. For example, www.bosch.com.
Refer to *Section  Keypad Programming of Path # Network Address, Path # Port Number, and Path # Poll Rate*, *42* and *Section  Path # Poll Rate, page 41*.

### Path # Port Number

| | |
|---|---|
| **Default** | 7700 |
| **Selection:** | 1 to 65535 |

This prompt specifies the destination port number for each of the four enhanced communication route path destinations.

**NOTICE!**
Whenever a network 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.

Refer to *Section  Keypad Programming of Path # Network Address, Path # Port Number, and Path # Poll Rate, page 42*.

### 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.

**NOTICE!**
If using **Network Addresses** as the communication means for UL 864 Commercial Fire applications (D9412GV4 and D7412GV4), program this parameter as necessary.

**NOTICE!**
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.

**NOTICE!**
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.

**NOTICE!**
The control panel readjusts a Heartbeat Poll rate of 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 the SDI paths. Refer to *Table 3.4, Page 25*.
For SDI2-2 (Path 1 = SDI 21, Path 2 = SDI 22, Path 3 = SDI 23, Path 4 = SDI 24).
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 3.14.2 Panel-Wide Relays, page 121*.

**Keypad Programming of Path # Network Address, Path # Port Number, and Path # Poll Rate D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **ENHANCED COMM** option. Press [ENT].
2. The keypad alternates between **COMMUNICATIONS>** and **ENHANCED> YES**. Press [NEXT] to access the **PATH 1 - 4** prompt.
3. Enter the path number you wish to configure and press [ENT]. The currently configured network address shows.
4. Press [ENT] to change the network address. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad only accepts byte numbers valid for the current prompt.

6. Repeat *Step 5* to enter the correct numbers for each byte.
7. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

8. The keypad shows the currently configured network address. Press [NEXT]. The currently configured port number shows.
9. Press [ENT] to change the port number.
10. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the port number and then enter the new port number.
11. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

12. Press [NEXT]. The currently configured path poll rate shows.
13. Press [ENT] to change the path poll rate.
14. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the poll rate then enter the new poll rate.
15. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Enhanced Comm** option. Press [ENT].
2. The **Enhanced Enabled** configuration shows, as does the **Select IP Path** option. Press the **Select IP Path** to access the **Path (1 – 4)** prompt.
3. Enter the path number you wish to configure and press [ENTER]. The currently configured network address shows.
4. Press the **Select IP Path** softkey to change the IP address. An editing cursor is enabled for the first byte.
5. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire IP address. Use the softkeys and the number buttons on the keypad to enter the new network address.

**NOTICE!**
The keypad only accepts byte numbers valid for the current prompt.

6. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

7. The keypad shows the currently configured network address and the **Port Number** option. Press the **Port Number** softkey. The currently configured port number shows.
8. Press the **Edit** softkey to change the port number.
9. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire network address. Use the softkeys and the number buttons on the keypad to enter the new port number.
10. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

11. When the keypad shows the currently configured port number and the **Poll Rate** option, press the **Poll Rate** softkey. The currently configured path poll rate shows.
12. Press the **Edit** softkey to change the path poll rate.
13. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire poll rate. Use the softkeys and the number buttons on the keypad to enter the new poll rate.
14. Press the **Save** softkey to save the changes. When the keypad reads **Parameter Saved**, your selection is configured.

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.

**Example of Heartbeat as shown in *Figure 3.1, Page 44*:**

– **Path # Poll Rate** is set to 120 sec
– **Path # Ack Wait** time is set to 1 sec
– **Path # Retry Count** is set to 3

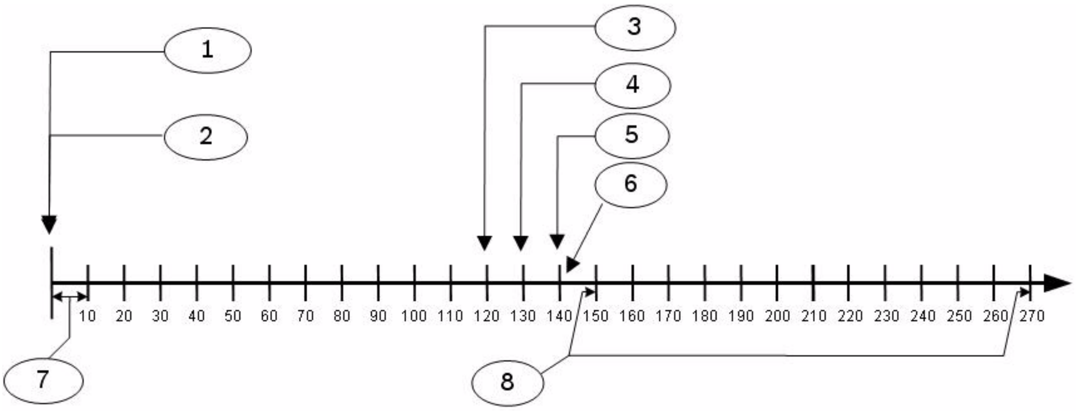


**Figure 3.1** Poll Rate Timeline

| Callout | Description |
|---|---|
| 1 | Heartbeat Poll sent |
| 2 | Acknowledgment received |
| 3 | Second Heartbeat Poll sent |
| 4 | No acknowledgment, Heartbeat re-sent, retry #1 |
| 5 | No acknowledgment, Heartbeat re-sent, retry #2 |
| 6 | Path declared failed |
| 7 | 10-sec interval |
| 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 SDI ## 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.

**NOTICE!**

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.

**NOTICE!**

5 min = 300 sec
1 hour = 3600 sec
12 hours = 43,200 sec
18 hours = 64,800 sec

**Path # Ack Wait**

| **Default** | 10 |
|---|---|
| **Selection:** | 5 sec to 65535 sec |
| 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.

**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 Heatbeat 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 RG8 SDI ###, SDI ###. Refer to *Table 3.4, Page 25* for valid SDI ### values.

**NOTICE!**

If using Network Addresses as the communication means for UL 864 Commercial Fire applications (D9412GV4 and D7412GV4), program this parameter as necessary.
The default settings meet or exceed the UL specifications.

### 3.4.1 Anti-Replay Security Feature

The Anti-Replay feature is enabled by default in the control panel and must be supported by the central station receiver.

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.

**Path # Enable Anti-Replay**

| **Default** | Yes |
|---|---|
| **Selection:** | Yes or No |
| Yes | The anti-replay protocol is expected on the central station receiver and will uniquely authenticate each event from the control panel. |
| No | The anti-replay protocol is not expected on the central station receiver. |

## 3.5 SDI RPS/Enhanced Communications Configuration

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 network interface module and RPS (version 5.13 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:

- Provide for local programming by a DX4010V2 Serial Interface Module.
- Provide remote programming by a Conettix DX4020 Network Interface Module, an ITSDX4020-G, or a B420-G.
- Provide enhanced route paths for event reporting through a network using a Conettix DX4020 Network Interface Module, an ITSDX4020-G, or a B420-G.

Although not listed in this section, RPS checks for the RPS passcode (refer to *Section 3.8 RPS Parameters, page 54*), Datalock Code, and control panel type to determine if this RPS session should continue.

## 3.5.1 Configuration for RPS Over Network

COMMAND 43 (Remote Programming) can establish control panel initiated communication with RPS over the phone or over the network. *Figure 3.2, Page 47* and *Figure 3.3, Page 48* show the structure of COMMAND 43.

### Answer RPS Over Network

| | |
|---|---|
| **Default** | Yes |
| **Selection:** | Yes or No |
| Yes | Enable automatic answer of RPS initiated sessions over the network. |
| No | Do not automatically answer RPS initiated sessions over the network. |

This prompt determines if the control panel automatically answers RPS initiated sessions through a network interface module on the SDI bus.

This prompt can be momentarily disabled by selecting ALLOW ANSWER through COMMAND 43 (Remote Programming) menu (refer to *Figure 3.2, Page 47* and *Figure 3.3, Page 48*).

**NOTICE!**

If the Reset switch (labeled S1) label is in the locked position, network RPS programming is allowed even if this prompt is set to **No**.

### RPS Address Verification

| | |
|---|---|
| **Default** | No |
| **Selection:** | Yes or No |
| Yes | Verifies that the incoming RPS network address matches the address entered in **RPS Network Address**. |
| No | Do not verify the RPS network address. Allow RPS to connect to the control panel from any network source . |

When enabled, this feature will verify that the Remote Programming Software connecting to the control panel is coming from a known IP address.

**NOTICE!**

If the Reset switch (labeled S1) label is in the locked position, network RPS programming is allowed even if this prompt is set to **No**.

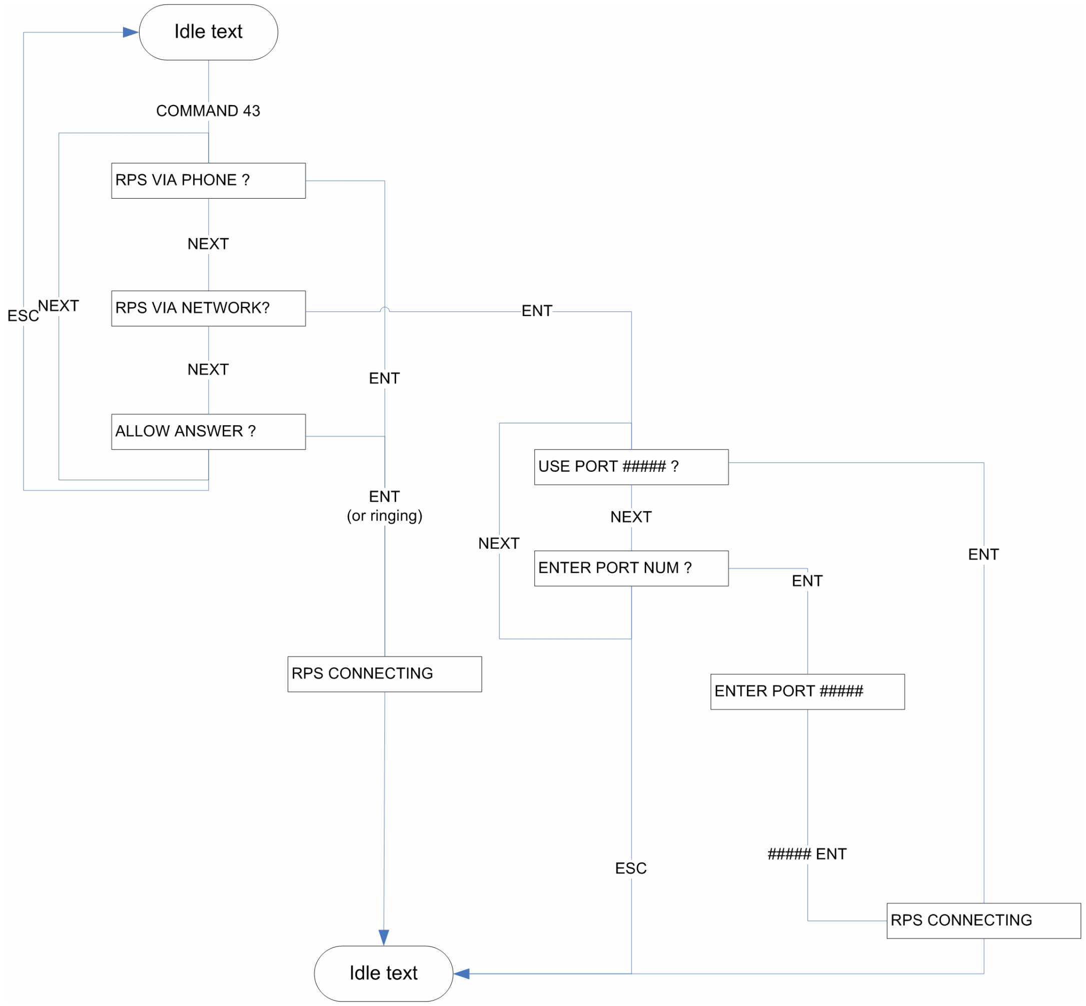


**Figure 3.2** COMMAND 43 Flow Chart (D1255)

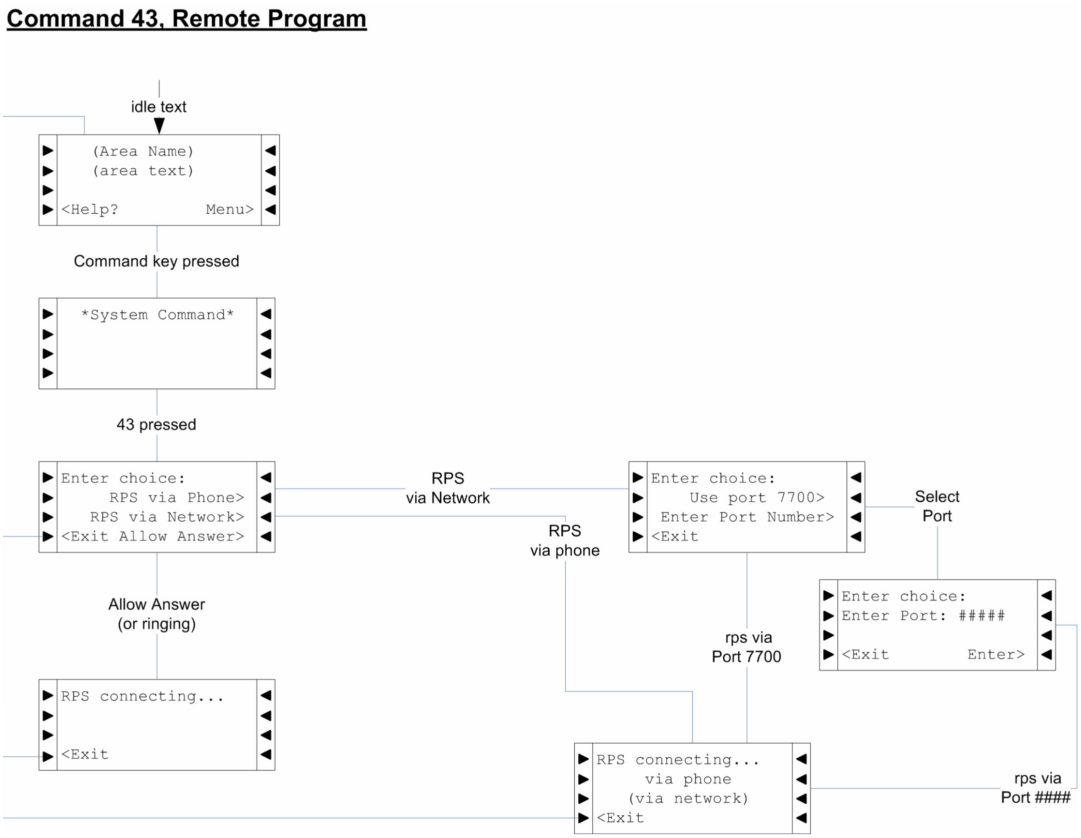


**Figure 3.3** COMMAND 43 Flow Chart (D1265)

### RPS Network Address

| | |
|---|---|
| **Default** | Blank |
| **Selection:** | 0.0.0.0 to 255.255.255.255 or [host name] |
| 0 to 255 | There are four numbers for an IPV4 address. Leading zeros are not required. A host name can be used if a B420 network communication module is installed on the control panel. |

This prompt contains the network host name or the IP address for RPS that the control panel uses to call RPS.

An IPv4 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. Contact your network administrator to determine the IP address to which the RPS computer is connected. If a B420 Ethernet Communication Module is installed, then the control panel has the option to use a host name (for example, *www.bosch.com*), for the RPS Network Address .

Refer to *Section RPS Network Address, page 48* and *Section RPS Port Number, page 48*.

### RPS Port Number

| | |
|---|---|
| **Default** | 7750 |
| **Selection:** | 1 to 65535 |

This prompt specifies the destination port for outgoing RPS session requests to the IP address specified in **RPS Network Address.**

### Keypad Programming of RPS Network Address and RPS Port Number D1255

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS PARAMETERS** option. Press [ENT]. The keypad shows the **RPS PASSCODE** option and the currently configured passcode.
2. Press [NEXT] twice to advance to the **RPS IP ADDRESS** option and press [ENT]. The currently configured IP address shows.
3. An invisible editing cursor is enabled for the first byte.
4. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad does not accept numbers 256 to 999.

5. Repeat Step 4 to enter the correct numbers for each byte.
6. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

7. When the keypad reads RPS IP ADDRESS, press [NEXT] to advance to the **RPS IP PORT** option. The keypad shows the currently configured port number.
8. Press [ENT] to change the port number.
9. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the port number and then enter the new port number.
10. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS Parameters** option. Press [ENTER]. The keypad shows the **RPS Passcode** option and the currently configured passcode.
2. Press **Phone Number** softkey. The keypad shows the currently configured phone number and the **IP Address** option.
3. Press the **IP Address** softkey. The currently configured IP address shows.
4. Press the **Edit** softkey to change the IP address.
5. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire IP address. Use the softkeys and the number buttons on the keypad to enter the new IP Address.

**NOTICE!**
The keypad does not accept invalid byte numbers.

6. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

7. When the keypad reads **RPS IP Address**, press the **Port Number** softkey. The keypad shows the currently configured port number.
8. Press the **Edit** softkey to change the port number.
9. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire port number. Use the softkeys and the number buttons on the keypad to enter the new port number.
10. Press the **Exit** softkey to save the changes.

## 3.6 Power Supervision

### AC Fail Time

| | |
|---|---|
| **Default:** | 1:00 |
| **Selection:** | 0:01 to 90:00 (minutes:seconds) |

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. AC power is continuously monitored by the control panel, any installed SDI2 bus Power Supply modules and any installed RF Repeaters. The response to this prompt is the actuation of the relay programmed in the Panel-Wide Relays prompt **AC Failure** (refer to *Section 3.14.2 Panel-Wide Relays, page 121*) and the AC Fail report enabled by the **AC Fail/Restoral** Report prompt. Local annunciation of an AC failure is controlled by the **AC Fail Display** prompt.

**NOTICE!**
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 (D9412GV4 and D7412GV4), program AC Fail Time with 1:00.
Always check with the Authority Having Jurisdiction for local requirements.

### Resend AC Fail

| | |
|---|---|
| **Default:** | No Responses |
| **Selection:** | No Responses, 6 hrs, 12 hrs |
| No Response | Only send the AC Fail report upon failure. |
| 6 hr | Send AC Fail report upon failure and every 6 hours after this while the failure persists. |
| 12 hr | Send AC Fail report upon failure and every 12 hours after this while the failure persists. |

This prompt controls the repeated transmission of the AC Failure report to the central station while the fault persists. **AC Fail/Restoral Report** must be set to **Yes**, and **AC Tag Along** must be set to **No** for this feature to work. This prompt applies to AC failure events generated by the control panel, any installed SDI2 bus power supply modules and any installed RF Repeaters.

**NOTICE!**
For the following items to be true, **AC Fail/Restoral Report** must be programmed as **Yes** and **AC Tag Along** must be programmed as **No**.

**NOTICE!**
To eliminate **AC Reporting**, **AC Tag Along** and **AC Fail/Restoral Report** must be programmed as No.

### 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. This prompt applies to AC failure events generated by the control panel, any installed SDI2 bus power supply modules and any installed RF Repeaters.

### AC Fail/Restoral Report

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |
| Yes | Send AC Fail and AC Restoral Reports. |
| No | Do 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**. This prompt applies to AC failure events generated by the control panel, any installed SDI2 bus power supply modules, and any installed RF repeaters.

### 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.

**NOTICE!**
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.

**NOTICE!**
AC **Tag Along** is required for NFPA and UL 864 Commercial Fire systems (D9412GV4 and D7412GV4). Be sure to program **AC Fail/Restoral Report** 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.

**NOTICE!**
To comply with NFPA standards and UL 864 requirements for Commercial Fire systems (D9412GV4 and D7412GV4), program this item as **Yes**.

**NOTICE!**
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  Command Center, page 79* for keypad configurations.

### Battery Fail/Restoral Report

| | |
|---|---|
| **Default:** | Yes |
| **Selection:** | Yes or No |

| | |
|---|---|
| Yes | Battery Failure and Restoral Reports are sent to the central station.<br>**Modem Reports**: Missing or shorted: BATTERY MISSING<br><br>Discharge below 12.1 VDC: BATTERY LOW |
| No | Battery Failure and Restoral Reports are not sent to the central station. |

This prompt enables a report to be sent when the control panel or an SDI2 bus power supply module detects a low or missing battery.

**NOTICE!**
To comply with NFPA standards and UL 864 requirements for Commercial Fire systems (D9412GV4 and D7412GV4), program this item as **Yes**.

## 3.7 Printer Parameters

Up to three D9131A Parallel Printer Interface Modules can be connected to a D9412GV4 (one printer for a D7412GV4 and a D7212GV4) SDI bus. Each printer is identified by an address of 17, 18, or 19. Options are available for Routing Reports and area assignments.

**P## Area Assign**

| | |
|---|---|
| **Default:** | 1 |
| **Selection:** | 1 to 32 for D9412GV4<br>1 to 8 for D7412GV4<br>1 to 4 for D7212GV4 |

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 **printers SDI** address. |
| No | More than one unsupervised printer can be installed using this **printers 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.

**NOTICE!**
Unsupervised printers sharing the same address setting print the same text.

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

**NOTICE!**
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.

**NOTICE!**
The printer cannot show area numbers greater than Area 8. When printed, Areas 9 and higher print as 00.

### 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. |

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

### P## A1 [through A#] 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.

**NOTICE!**
Refer to the report tables in *Section 3.3 Routing, page 23* 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:** | Yes (Printer 1 only) |
| **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:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

### P## Access Event

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

### P## User Event

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

### P## Test Event

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

### P## Diag Event

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

**P## Auto Functions Event**

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

**P## RPS Event**

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

**P## Relay Event**

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

**P## Point Event**

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

**P## User Chng Evt**

| | |
|---|---|
| **Default:** | Yes (Printer 1 only) |
| **Selection:** | Yes or No |

## 3.8 RPS Parameters

Use these program items to enable remote programming software (RPS) functions in the control panel using the on-board phone connection or a Network Interface Module. Refer to *Section 3.5 SDI RPS/Enhanced Communications Configuration, page 45* for more information on these types of remote programming.

### 3.8.1 Uploading and Downloading Reports

If the control panel is programmed to send reports in ModemIIIa$^{2}$ reporting format, when RPS contacts the control panel and the passcode is incorrect, the control panel sends an RPS Access Fail Report to the central station receiver. 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 central station receiver, 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 central station receiver.

When RPS programming changes parameters, a Parameters Changed Report is sent to the central station receiver. If any programming changes are made, click the **Reset Panel** check box and click **OK**.

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 0 in the **Answer Armed** and **Answer Disarmed** prompts in this section.

### 3.8.2 Log Threshold Reports

When the event log reaches the percentage configured in **Log % Full** and the control panel is properly configured, it will contact Unattended RPS over phone or network.

If communication with RPS is unsuccessful, or if not properly configured, the control panel generates Log Threshold and Fail to Call RPS events.

Fail to Call RPS Events are logged only locally. If properly configured, the control panel makes multiple attempts to reach RPS before sending the reports. To enable transmission of the events when the Log Threshold is reached, set a valid phone number in **RPS Phone Number** (refer to *Section RPS Phone #, page 58*) or set a valid IP address in **RPS Network Address** (refer to *Section RPS Network Address, page 48*).

### 3.8.3 Panel Initiated Unattended RPS

The control panel will automatically contact Unattended RPS when the Log Threshold is reached or when the Contact RPS Sked function is executed. When the control panel is attempting to contact Unattended RPS, it will start with two attempts. 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 contacting Unattended RPS 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 Fail to Call RPS Report and abandoning the effort.

If network RPS is configured, then any control panel initiated attempt to contact Unattended RPS will be over network. If network RPS is not configured, then contact will be attempted over the phone.

**Manually Initiated Unattended RPS**: If properly configured, an authorized user can initiate contact with Unattended RPS by entering [COMMAND][4][3] and advancing the menu until RPS via Phone or RPS via Network shows. After proceeding through one of these options, the control panel makes one attempt to contact Unattended 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.

**Keypad Programming of RPS Passcode**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS PASSCODE** option. The keypad shows the currently configured passcode.
2. Press [ENT] to change the passcode. An invisible editing cursor is enabled.
3. The [PREV] button acts as a [Backspace] key. The [COMMAND] key allows you to cycle though the special passcode characters (A, B, C, D, E, F); the [NEXT] key selects the passcode character. Press [PREV] to delete the characters of the passcode, and then enter the passcode.
4. Press [ENT] to save the passcode. When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS Parameters** option and press [ENTER]. The keypad shows the currently configured RPS Passcode.
2. Press the **Edit** softkey to change the passcode. An editing cursor is enabled.
3. Use the softkeys and the number buttons on the keypad to enter the new passcode. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire passcode. When entering a letter character, press the letter's softkey to select

it. The **Previous** and **Next** softkeys advance through the letter characters (A, B, C, D, E, F).

4. Press the **Save** softkey to save the passcode. When the keypad reads **Parameter Saved**, your selection has been configured.

**Log % Full**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 to 99 |

When the event log reaches the percentage full indicated in this prompt, the control panel logs a Log Threshold event. If **Contract RPS if Log % Full** is set to **Yes**, then the control panel will attempt to contact Unattended RPS and copy the event log before messages are overwritten.

A setting of 0 disables the Log Threshold and Log Overflow Events. These events are not entered in the log or reported to the central station receiver or the local printer.

The control panel continues to log events after the Log Threshold Report is sent. When the event log reaches 100%, a Log Overflow event is generated and the oldest events are overwritten.

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.

**NOTICE!**

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

**NOTICE!**

Failure to program the RPS telephone number and the RPS IP address number results in a FAIL TO CALL RPS trouble event sent to the central station when the log threshold is reached. Refer to *Section  RPS Phone #, page 58* for information about programming the RPS telephone number. Refer to the *Section  Path # Network Address, page 41* for information about enabling network RPS.

**Contact RPS if Log % Full**

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |
| Yes | Directs the control panel to automatically communicate with Unattended RPS over network or phone when Log Threshold is reached. |
| No | The control panel will not automatically contact RPS when Log Threshold is reached. |

When the event log reaches the percentage full indicated by **Log % Full** the Log Threshold event is put in the event log. If this prompt is set to Yes and either the **RPS Network Address** or **RPS Phone #** are programmed, then the control panel will attempt to contact Unattended RPS as described in *Section 3.8.3 Panel Initiated Unattended RPS, page 55*.

**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 *Section  RPS Phone #, page 58*). This ensures that the control panel only communicates with RPS units connected to the programmed phone number.<br>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.

**NOTICE!**
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.

**NOTICE!**
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.

**NOTICE!**
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:** | 7 |
| **Selection:** | 0 to 15 |
| 0 | 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.

**NOTICE!**
For the purposes of answering the RPS phone call, the control panel considers Perimeter Armed a disarmed state.

### Answer Disarmed

| **Default:** | 7 |
|---|---|
| **Selection:** | 0 to 15 |
| 0 | |
| 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.

**NOTICE!**
For the purposes of answering the RPS phone call, the control panel considers Perimeter Armed a disarmed state.

### RPS Phone #

| **Default:** | Blank |
|---|---|
| **Selection:** | Blank or up to 24 characters |
| Blank | Control panel does not dial a phone number for RPS. |
| 1 to 24 characters | Enter up to 24 characters to define dialing characteristics. |

This is the phone number the control panel dials to contact RPS. Refer to *Section 3.8.1 Uploading and Downloading Reports, page 54* for instructions on configuring special phone number digits to detect dial-tone detect and to pause dialing. The control panel dials this number when any of the following events occur:

- Log % Full threshold is achieved.

**NOTICE!**
If Log % Full is programmed with a value (1 to 99) and an RPS phone number or RPS IP address are programmed, the control panel attempts to communicate with Unattended RPS when the log threshold is reached.

- The control panel is contacted by RPS and RPS Call Back is programmed Yes.
- The user enters and selects the call RPS option from the menu. On the D1255:
  - 1. Press [COMAND][4][3].
  - 2. Press [NEXT] until RPS via Phone? appears, then press [ENTER].

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

Refer to *Section 3.5 SDI RPS/Enhanced Communications Configuration, page 45* for other connection methods.

**NOTICE!**
Refer to *Section  Phone #, page 17* descriptions of special programming values for the RPS Phone number.

**Keypad Programming of RPS PHONE #**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS PARAMETERS** option. Press [ENT]. The keypad shows the **RPS PASSCODE** option and the currently configured passcode.
2. Press [NEXT] to advance to the **RPS PHONE NUMBER** option.
3. The keypad shows the currently configured phone number. Press [ENT] to edit the phone number.
4. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the phone number, and then enter the new phone number.
5. Press [ENT] to save the phone number. When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **RPS Parameters** option. Press [ENTER]. The keypad shows the **RPS Passcode** and the currently configured passcode.
2. Press **Phone Number** softkey.
3. The keypad shows the currently configured phone number.
4. Press the **Edit** softkey to change the phone number.
5. The **Pause** and **DT Detect** (Dialtone Detect) softkeys enter special characters. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire phone number. The [COMMAND] and [ENTER] keys allow you to enter an * or a #. Use the softkeys, the number buttons, and the [COMMAND] and [ENTER] keys on the keypad to enter the new phone number.
6. Press [ENT] to save the phone number. When the keypad reads **Parameter Saved**, your selection has been configured.

**RPS Modem Speed**

| | |
|---|---|
| **Default:** | 1200 |
| **Selection:** | 300, 1200, 2400 |

Select the baud rate for RPS-to-control panel communication when using a PSTN connection.

## 3.9 Miscellaneous

**Duress Type**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1, 2, or 3 |
| 0 | Do not send a duress event with any passcode. |
| 1 | Increase the last digit by 1 to generate an alarm. For example, if the passcode is 6123, 6124 activates a duress alarm.<br>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.<br>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. |

| | |
|---|---|
| 2 | Increase the last digit by 2 to generate an alarm. For example, if the passcode is 6123, 6125 activates a duress alarm.<br>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.<br>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. |
| 3 | Send a Duress event when any Passcode with **L# Send Duress** set to **Yes** is entered. |

This program item determines when a passcode entry with **L# Send Duress** authority should produce a duress alarm.

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

**NOTICE!**
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:** | Yes |
| **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 Duress Type** this prompt must be set to **Yes**.

### Call for Service Text

| | |
|---|---|
| **Default:** | "Contact your dealer" |
| **Selection:** | Twenty alphanumeric characters |
| Enter the text to display on a D1260 series keypad when the control panel is out of service. | |

### On-site Authorization for Firmware Update

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |
| Yes | Authorized personnel on-site must enter the authorization code at one of the command centers at the designated time during the remote firmware update process. |
| No | No on-site authorization is required. |

Perform firmware updates using RPS. *RPS Online Help* includes instructions for using the Firmware update feature.

**NOTICE!**
It is recommend that a full system test be performed whenever firmware is updated locally or remotely.

## 3.10 Area Parameters

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

### 3.10.1 Area Parameters

Enter the area number you are programming.

**Area# 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.

Refer to *Section  Keypad Programming of Area # On and Area# Account Number, page 61*.

**NOTICE!**

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.

**NOTICE!**

To meet UL 864 requirements (D9412GV4 and D7412GV4), set **A# Area On** to **Yes**.

**Area# Account Number**

| | |
|---|---|
| **Default:** | 0000 |
| **Selection:** | For Modem format and Contact ID (four-digit account numbers): 0000 to 9999, BBBB to FFFF<br>For Modem format (ten-digit account numbers): 0000000000 to 9999999999, BBBBBBBBBB to FFFFFFFFFF |

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 IIIa$^2$**: Enter a four-digit or ten-digit number.

**Keypad Programming of Area # On and Area# Account Number**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **AREA PARAMETERS** option. Press [ENT].
2. The keypad reads **AREA NUM 1 – 32** (1 – 8 for the D7412GV4).
3. Enter the area number you wish to configure and press [ENT]. The current area status shows (for example, AREA 1 ON: YES).
4. Press [ENT] to change the area’s status.

5. Press the [PREV] or [NEXT] button to toggle between YES and NO, and then press [ENT] when the desired configuration option shows.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

6. When the keypad reads **AREA STATUS**, press [NEXT] to advance to the **A# ACCOUNT NUMBER** option. The keypad shows the currently configured account number.
7. Press [ENT] to change the account number.
8. The [PREV] button acts as a [Backspace] key. The [COMMAND] key cycles though the special account number characters (B, C, D, E, F); [NEXT] select the account number character. Press [PREV] to delete the characters of the account number and then enter the new account number.
9. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection is configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Area Parameters** option. Press [ENT].
2. The keypad reads **Area Number 1 – 32** (1 - 8 for D7412GV4 and 1 - 4 for D7212GV4).
3. Enter the area number you wish to configure and press [Enter]. The current area status shows (for example, Area 1 On: Yes).
4. Press the **Edit** softkey to change the area’s status.
5. Press the **Yes** or **No** softkey, and then press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

6. When the keypad reads **Area Status**, press the **Account Number** softkey. The keypad shows the currently configured account number.
7. Press the **Edit** softkey to change the account number.
8. Use the softkeys and the number buttons on the keypad to enter the new account number. The **Backspace** softkey allows you to erase characters. The Clear softkey allows you to clear the entire account number. When entering a letter character, press the letter's softkey to select it. The **Previous** and **Next** softkeys advance through the letter characters (A, B, C, D, E, F).
9. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection is configured.

### Area# Force Arm/Bypass Max

| | |
|---|---|
| **Default:** | 2 |
| **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## Force Arm Returnable** and **P## Bypass Returnable** in *Section P## Force Arm Returnable, page 140* and *Section P## Bypass Returnable, page 140* for returning a point to the system when the point returns to normal or when the area is disarmed.

**NOTICE!**

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.

### Area# Delay Restorals

| | |
|---|---|
| **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.

**NOTICE!**
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 Delay Time**

| | |
|---|---|
| **Default:** | 60 sec |
| **Selection:** | 0 to 600 (in 5 sec increments) |

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

**NOTICE!**
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. |

**NOTICE!**
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.

**NOTICE!**
- **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 5.1 Point Index, page 130*. 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 or 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 3.15* for an example of **Verify Time**.

| | **Verification Point Activation** | **Verify Time/ Reset Sensors** | **60 sec Confirmation** | **Restart Alarm Verification Cycle if an Alarm Verification point activates** |
|---|---|---|---|---|
| | | Power removed, ignore activity | Generate alarm if additional activity received | |
| **Example:** Total Cycle time 80 sec | * | 20 sec | 60 sec | |

**Table 3.15** Verify Time

**NOTICE!**

To meet UL 864 requirements (D9412GV4 and D7412GV4), set **A# Verify Time** to **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 3.9 Miscellaneous, page 59* for an explanation of duress.

**For SIA CP-01 Compliance**:

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

**CAUTION!**

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.

### A# Area Type

| | |
|---|---|
| **Default:** | Regular |
| **Selection:** | Regular, Master, Associate, Shared |

**Regular**

Arms or disarms as an independent area.

**Master**

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.

A master area can be disarmed regardless of the armed state of the other areas in the account.

Multiple master areas can be programmed in a single account.

**NOTICE!**

**CC# Scope** affects master arming.

**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.

**NOTICE!**

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 *Section 3.10.4 Open/Close Options, page 69*) occurs before all associate areas are armed

**Associate**

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.

**NOTICE!**

Keypads assigned to associate areas, when used with shared areas, must have **CC# Scope** programmed.

**Shared**

- Is not associated to other areas by account number, they are shared panel wide.
- Are armed when all Associate areas in the control panel are Master Delay armed.
- Are disarmed when at least one Associate area in the control panel is taken out of Master Delay armed state.
- Cannot be individually armed using a passcode, key switch, keyfob, sked, or RPS.

**NOTICE!**

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 Associate areas. Shared areas associate with all Associate areas regardless of their account assignments. The shares area does not begin to arm until all Associates finish arming.

## 3.10.2 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.

**NOTICE!**
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 restarts 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 control section), both the associate area and shared area disarms when the token or card is presented. (Refer to *Section  Access Control Readers Assigned to the Shared Area, page 66*.)

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

### 3.10.3 Bell Parameters

The D9412GV4 and the D7412GV4 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 3.14.1 Area Relays, page 118*.

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**.

### 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.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), 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 Pattern

| | |
|---|---|
| **Default:** | Pulse |
| **Selection:** | Steady, Pulse, CA Standard, TempCode3 |
| Steady | Steady Output |
| Pulse | Pulse March Time<br>120 beats per minute, at an even tempo |
| CA Standard | California Standard<br>10 sec On + 5 sec Off + 10 sec On + 5 sec Off. This sequence repeats until bell time expires. |
| TempCode3 | Temporal Code 3<br>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 ± 10% tolerance. |

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

**NOTICE!**
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 min to 90 min (in one-minute increments) |

ⓘ **NOTICE!**
For D9412GV4 and D7412GV4 Control Panels, use:
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.

ⓘ **NOTICE!**
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 Pattern

| | |
|---|---|
| **Default:** | Steady |
| **Selection:** | Steady, Pulse, CA Standard,TempCode3 |
| Steady | Steady Output |
| Pulse | Pulse March Time<br>120 beats per minute, at an even tempo |
| CA Standard | California Standard<br>10 sec On + 5 sec Off + 10 sec On + 5 sec Off. This sequence repeats until bell time expires. |
| TempCode3 | Temporal Code 3<br>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 ± 10% tolerance. |

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

### 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.

ⓘ **NOTICE!**
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.

**NOTICE!**
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.

**NOTICE!**
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.

## 3.10.4 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.

**NOTICE!**
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.

**NOTICE!**
For the scheduled suppression of Opening and Closing Reports, refer to *Section 6.1.1 Opening and Closing, page 154*) 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# Account 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# Account O/C feature. To use these features, program O/C Windows.

### A# Account O/C

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |

| | |
|---|---|
| Yes | Send Opening and Closing Reports by account.<br>Use this selection if the control panel sends reports to an automation system that cannot interpret multiple Area Opening and Closing Reports.<br>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.<br>**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).

**NOTICE!**

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 | Do not send Opening and Closing Reports to the central station if they occur inside an active window.<br>If an Opening or Closing Report occurs outside a window, send it with an early or late modifier. Refer to *Section 6.1.1 Opening and Closing, page 154*.<br>The active window must be a Closing Window for Closing Reports. It must be an Opening Window for Opening Reports. |
| No | 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.<br>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. |

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 | The area automatically master arms at the end of the Close Window. When the area is armed automatically, a Closing Report is sent if the Area or Account Reports are programmed to do so. |
| 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.

**NOTICE!**

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.<br>**Note:**<br>Program an exit delay time in **Exit Dly Time**. |
| No | Fail to Close Report is not sent for this area.<br>– If **Auto Close** is programmed **Yes**, a Fail to Close Report is sent because it occurs when the Closing Window stop time occurred.<br>– 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# 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.

**NOTICE!**
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).

### A# Restricted 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.<br>**Note:**<br>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.<br>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.<br>Regardless of programming in Authority Levels **L## Restricted O/C**, reports are not restricted in this area when this item is programmed as No.<br>**Note:**<br>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 *Section L## Perimeter O/C, page 113*.

**NOTICE!**

This reporting requires ModemIIIa$^2$ reporting format reporting. Some central station automation systems cannot process these reports.

## 3.10.5 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. |

**NOTICE!**
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.

**NOTICE!**
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.

**NOTICE!**
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.

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

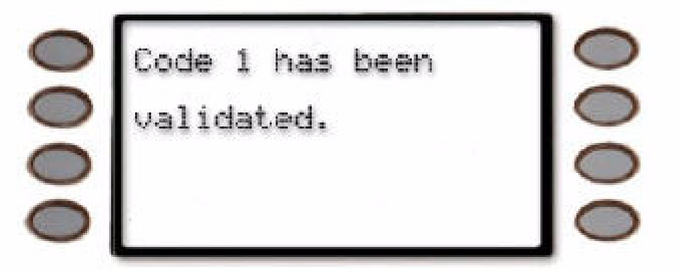
**NOTICE!**
To avoid unintended results for the end user of the system:

- 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**.

**NOTICE!**
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.

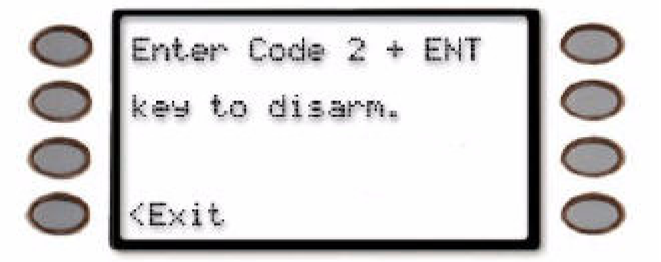
**D1255 Keypad**
After the first valid passcode is entered, the D1255 replaces the scrolling DISARM NOW and the Point Text display with the SECOND CODE:.display
When the user presses the first digit of the second code, the display changes to SECOND CODE: *.
SECOND CODE: appears for 19 sec. If no digits 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.



```
Code 1 has been
validated.
```

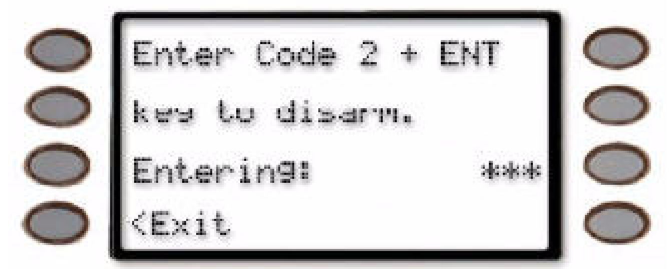
Then the next message appears requesting a second code.



```
Enter Code 2 + ENT
key to disarm.

<Exit
```

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



```
Enter Code 2 + ENT
key to disarm.
Entering:       ***
<Exit
```

**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 *Section  Early Ambush Timer, page 176*.<br>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.

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

Code 2 has been
validated. Window
cancelled.
Have a nice day!

**Parameter Setup Requirement:**

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

**NOTICE!**

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 *Section  Secondary Ambush Code, page 176* for information about the unique behavior of the two passcodes.

**For SIA CP-01 Compliance:**

**NOTICE!**

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

**A# Exit Delay 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. |

**NOTICE!**

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.

**NOTICE!**

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:** | No |
|---|---|
| **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.

**NOTICE!**

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

**For SIA CP-01 Compliance**

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

**A# Exit Warning**

| **Default:** | No |
|---|---|
| **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 out 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.

**NOTICE!**

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 Warning** must be set to **Yes**.

**A# Entry Warning**

| **Default:** | No |
|---|---|
| **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**.

## 3.11 Keypad (Command Center)

This programming module contains three programming categories: Command Center Assignments, Area Text, and Custom Function.

**Command Center**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Default:** | 1 | | | | | |
| **Selection:** | 1 to 16 for D9412GV4 and D7412GV4<br>1 to 8 for D7212GV4 | | | | | |
| DIP Switch Setting | | | | | | |
| SDI Address (CC#) | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | ON | ON | ON | ON | | ON |
| 2 | OFF | ON | ON | ON | | ON |
| 3 | ON | OFF | ON | ON | | ON |
| 4 | OFF | OFF | ON | ON | | ON |
| 5 | ON | ON | OFF | ON | | ON |
| 6 | OFF | ON | OFF | ON | | ON |
| 7 | ON | OFF | OFF | ON | | ON |
| 8 | OFF | OFF | OFF | ON | | ON |
| 9 | ON | ON | ON | OFF | | ON |
| 10 | OFF | ON | ON | OFF | | ON |
| 11 | ON | OFF | ON | OFF | | ON |
| 12 | OFF | OFF | ON | OFF | | ON |
| 13 | ON | ON | OFF | OFF | | ON |
| 14 | OFF | ON | OFF | OFF | | ON |
| 15 | ON | OFF | OFF | OFF | | ON |
| 16 | OFF | OFF | OFF | OFF | | ON |
| Enter the keypad (CC) number for the SDI address you are programming. This number corresponds to the DIP switch address settings shown.<br>Switch 5: On=Encoding Tone On (default), Off=Encoding Tone Off | | | | | | |

## 3.11.1 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 sixteen 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.

Enhanced keypads (D1260 Series) and standard keypads (D1255 Series) cannot share the same SDI Address.

**NOTICE!**

The D1255 can be addressed as 1 through 16. The D1260 can be addressed only as 1 – 8.

**CC# Supervised**

| | |
|---|---|
| **Default:** | No |
| **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.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7212GV4), set **CC# Supervised** to **Yes** for the fire annunciation keypad.

**NOTICE!**
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.

**NOTICE!**
When this prompt is **Yes**, you cannot have duplicate DIP switch settings.

### CC# Enhanced Command Center

| | |
|---|---|
| **Default:** | No (Yes for Keypad 8) |
| **Selection:** | Yes or No |
| Yes | This keypad is a D1260 Series Keypad. |
| No | This keypad is not a D1260 Series Keypad. |

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

**Keypad Programming of CC# Enhanced Command Center**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **COMMAND CENTER** option.
2. Press [ENT]. The **CC NUM 1 – 16** option shows.
3. Enter the keypad number you wish to configure and press [ENT]. The keypad reads **CC# SCOPE**, and then the current configuration (for example, PANEL WIDE).
4. Press [NEXT]. The current keypad type shows (for example, CC - 1 TYPE ENHANCED: YES).
5. Press [ENT] to change the keypad's type.
6. Press [NEXT] or [PREV] to toggle to **No** to indicate that the D1255 is not an enhanced keypad, and then press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Command Center** option.
2. Press [ENTER]. The **CC Num 1 – 16** option shows.
3. Enter the keypad number you wish to configure and press [ENTER]. The keypad reads **CC# Scope**, and then the current configuration (for example, Panel Wide).
4. Press the **Type** softkey. The current keypad type shows (for example, CC (1) Type Enhanced: Yes).
5. Press the **Edit** softkey to change the keypad's type.
6. Press the **Yes** or **No** softkey, and then press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection has been configured.

**NOTICE!**
Reboot the system to enable a D1260 Series 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# Area Assign

| | |
|---|---|
| **Default:** | 1 |
| **Selection:** | 1 to 32 on D9412GV4<br>1 to 8 on D7412GV4<br>1 to 4 on D7212GV4 |

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

### CC# Scope

| | |
|---|---|
| **Default:** | No Keypad (Panel Wide for keypads 1 and 8) |
| **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# Account 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. (This option is not available through Keypad Programming.) |
| 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.

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

**NOTICE!**
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 A#] in Scope**. Before exiting from a custom program, check each area and ensure that it is enabled and disabled correctly.

### CC# A1 (through A#) in Scope

| | |
|---|---|
| **Default:** | None (All for Keypads 1 and 8) |
| **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 areas and doors are included in the scope of this keypad for viewing status, arming or disarming, and controlling doors from the keypad.

**Keypad Programming of CC# Scope**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **COMMAND CENTER** option.
2. Press [ENT]. The **CC NUM 1 – 16** option shows.
3. Enter the keypad number you wish to configure and press [ENT]. The keypad reads **CC# SCOPE**, and then the current configuration (for example, PANEL WIDE).
4. To change the configuration, press [ENT] when the current configuration shows, and then press [NEXT] or [PREV] to scroll through the options, as listed in *Section CC# Scope, page 81*.
5. When the keypad reads the desired configuration option, press [ENT] to select it. When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Command Center** option.
2. Press [ENTER]. The CC Num 1 – 16 option shows.
3. Enter the keypad number you wish to configure and press [ENT]. The keypad reads **CC# Scope**, and then the current configuration (for example, Panel Wide).
4. To change the configuration, press the **Edit** softkey, and then press the **Next** or **Previous** sofkeys to scroll through the options, as listed in *Section CC# Scope, page 81*.
5. When the keypad reads the desired configuration option, press the **Save** softkey to select it.

When the keypad reads **Parameter Saved**, your selection has been configured.

**CC# Passcode Follows Scope**

| | |
|---|---|
| **Default:** | Yes |
| **Selection:** | Yes or No |
| Yes | 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.<br>– 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.<br>– 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 | 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. |

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.

**NOTICE!**
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.

**NOTICE!**
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# Enter Key Relay

| **Default:** | 0 |
|---|---|
| **Selection:** | 0 to 128, A, B, C for D9412GV4<br>0 to 64, A, B, C for D7412GV4<br>0 to 24, A, B, C for D7212GV4 |
| 0 | The [ENTER] key is not used to activate a relay. |
| 1 to 128 (64, 24), A, B, C | Assign the relay number that activates when [ENTER] is pressed at this keypad after the user enters a valid passcode. |

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.

- With **CC## Passcode Function** is set to **Cycle Relay**, entering a valid code and pressing [ENTER] at a keypad silences a ringing bell.
- Using the relay programmed in **CC# Enter Key Relay** for a low-level access control strike on a door does not shunt a point.

**NOTICE!**
When **CC## Passcode Function** is set to **Cycle Relay**, the keypad cannot be used to passcode arm or disarm.
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# Pass Code Enter Function

| **Default:** | Arm/Disarm |
|---|---|
| **Selection:** | Arm/Disarm, Cycle Door (D9412GV4/D7412GV4), Cycle Relay, Auto Re-arm |
| Arm/Disarm | Pass Code followed by ENTER (or ENT) key will start Master Delay Arm for all areas within the users authorized scope if the current area is disarmed. If the area is not disarmed, then all authorized areas will be disarmed. |
| Cycle Door | Pass Code followed by [ENTER] (or [ENT]) key will cycle the door programmed in CC# Assign Door, then will actuate the users authorized post access operations (Disarm, Perimeter Instant arm, or execute a Custom Function) if enabled. |

| | |
|---|---|
| Cycle Relay | Pass Code followed by [ENTER] (or [ENT]) key will momentarily activate the CC# Enter Key Relay for 10 seconds. |
| Auto Re-arm | Pass Code followed by [ENTER] (or [ENT]) key will restart Master Delay Arm for all areas within the users authorized scope if the current area is not disarmed. If the area is disarmed, then the arm state does not change. |

**For SIA CP-01 Compliance**

**CC# Passcode Enter Function** must be left at its default value **Arm/Disarm**.

### CC# Dual Authentication (D9412GV4/D7412GV4 Only)

This parameter enables or disables the Dual Authentication feature. With Dual Authentication, a user must enter a passcode AND present a credential to a card reader to gain access through a door.

**NOTICE!**

Users cannot use a key fob as the second method of authentication when Dual Authentication is enabled.

**NOTICE!**

Dual Authentication applies to **CC## Passcode Enter Function** settings of Arm/Disarm, Arm Cycle Relay, Cycle Door, and Auto Re-arm. When Dual Authentication is enabled, user commands (for example, CMD 43), require a passcode only.

Enabling Dual Authentication:

- Set the keypad’s configuration option of **Command Center Dual Authentication** to **Yes**.
- Set the keypad’s configuration option of **Command Center Assign Doo**r to the number of the door.
- Set the associated door’s configuration option of **Access Control CommandCenter # Scope** to the number of the keypad.
- Review the areas listed in the configuration option **Command Center Area(s) in Scope** for the keypad associated with the door. Ensure the doors **Access Control Entry Area** is included in the area list.
- **A# Two Man Rule** and **A# Early Ambush** must be disabled in the **D# Entry Area** for the **CC# Assign Door**.

If any of these conditions are not met, then the Passcode Function operates with single passcode authentication regardless of the setting of the **CC# Dual Authentication** prompt.

**For SIA CP-01 Compliance**

**CC# Dual Authentication** must be left at its default value **No**.

### CC# Dual Authentication Duration

| | |
|---|---|
| **Default:** | 10 sec |
| **Selection:** | 10 to 45 (in 5-sec increments) |

This is the amount of time allowed between the presentation of the user’s credentials to the reader and the entry of the user’s passcode at the keypad. If this time elapses, the Dual Authentication process is reset and authentication is denied.

### CC# Assign Door

| **Default:** | Door 1, Area 2 to 8 No Door |
|---|---|
| **Selection:** | No Door, 1 to 8 on D9412GV4<br>(No Door, 1 to 2 on D7412GV4) |
| No Door | No door controller is assigned for adding tokens. |
| 1 to 8 | The door controller assigned to this keypad is used to read new door credentials or when Dual Authentication is enabled. |
| This feature is not available with the D7212GV4. Keep the default setting. | |

The door assigned to this keypad is used:

- To add door credentials to a user
- With **CC## Close Door Warning Tone** to annunciate the **Door Left Open** warning
- To enable **CC# Dual Authentication** for **CC# Passcode Functions**.

**NOTICE!**

- 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 Access Control section, 9210 NOT READY appears at this keypad when you attempt to add a user or perform dual authentication.
- 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.
- The setting of **CC# Passcode Function** does not affect the ability to add or change door credentials.

**NOTICE!**

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).

**NOTICE!**

To meet UL 864 requirements (D9412GV4 and D7412GV4), set **CC# Trouble Tone** to **Yes**.

**NOTICE!**

Panel-wide trouble tones do not include Point Troubles, Buzz on Fault, or (for D9412GV4 and D7412GV4) Close Door Now.

**NOTICE!**

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.

**NOTICE!**
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**.

**NOTICE!**
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.

**NOTICE!**
This SIA CP-01 required feature is not supported on the D720 Series Keypads.

**NOTICE!**
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 Warning Tone

| | |
|---|---|
| **Default:** | Yes |
| **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 Warning Tone

| | |
|---|---|
| **Default:** | Yes |
| **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.. |
| This feature is not available with the D7212GV4. Keep the default setting. | |

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**.

### 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.

**NOTICE!**

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, 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. |

**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 REPORT SENT display message when an alarm is canceled after transmission occurs. To show this message, **Cancel Report** must be set to **Yes**. Refer to *Section 3.9 Miscellaneous, page 59*.

**For SIA CP-01 Compliance**

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

## 3.11.2 Area Text

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

**NOTICE!**

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# 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 an no points are faulted.

**Area# Account 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 ACCOUNT IS ON text appears at all keypads assigned to these areas, if more than one area has the same account number. The ACCOUNT IS ON text also appears if only one area in the system is used. Refer to the prompts **CC# Area Assign** and **Area # Account Is On** in *Section 3.11.1 Keypad (Command Center) Assignment, page 79*. When all areas in the account are master armed, the Area # Is On text is replaced by the ACCOUNT IS ON text if the area is armed before all other areas with the same account number.

**Blank Entry**

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

**Unique ACCOUNT IS ON Text**

Each area can have unique ACCOUNT 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 Series Keypad**

Although it is not programmed in this area, the D1260 Series 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 **Account # 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.

**Area# Name Text**

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **Selection:** | Sixteen alphanumeric characters |
| Enter the text for this area's name. This text only displays on the D1260 series keypads. | |

## 3.11.3 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 3.13 Function List, page 116*) 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 3.12 User Interface, page 93*, 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 *Section  M## CC Address 1 [through #], page 117*). If the Custom Function is not assigned to a specific keypad address, it does not appear in the menu.

**Custom Function**

| | |
|---|---|
| **Default:** | Blank |
| **Selection:** | Blank, 128 to 143 (on D9412GV4), 128 to 131 (on D7412GV4/ D7212GV4) |

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

**NOTICE!**

Custom Functions 132 through 143 are not available with the D7412GV4 and D7212GV4.

**CF### Text**

| | |
|---|---|
| **Default:** | Blank |
| **Selection:** | Sixteen alphanumeric characters. See *Section 3.11.2 Area Text, page 88* 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.

**NOTICE!**
Custom Functions 132 through 143 are not available with D7212GV4.

**CF### Key Strokes**

| | | | |
|---|---|---|---|
| **Default:** | Blank | | |
| **Selection:** | Up to 32 characters: 0 to 9, A, B, C, D, EBlank = disabled. | | |
| **Selection:** | **D1255 Key** | **D1255 Faceplate Labe**l | **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.

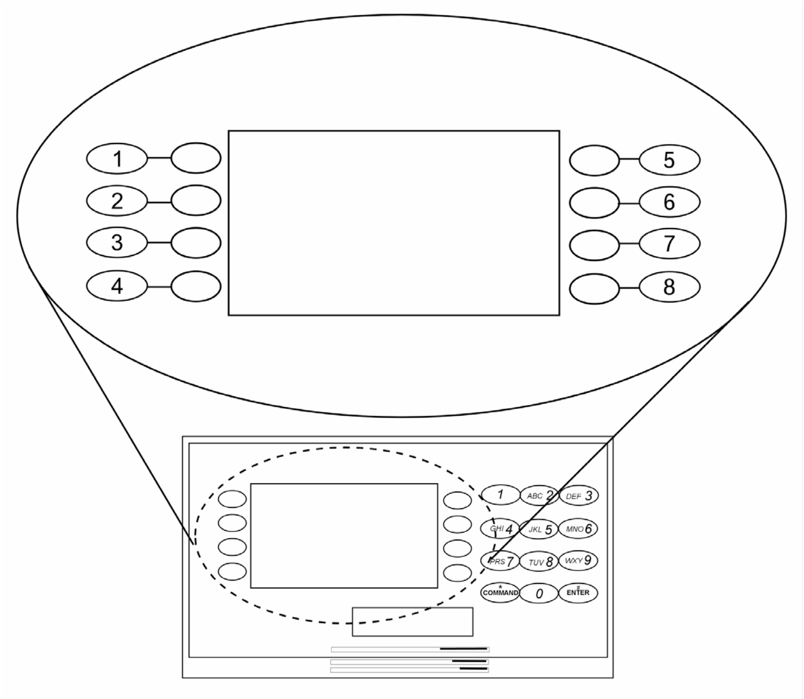


**Figure 3.4** Softkey Locations on the D1260 Keypad

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

**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.

| | Command | Keystrokes |
|---|---|---|
| 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 |

**Table 3.16** CF### Custom Function Keystrokes

- When **CF### Custom Function** is programmed with P, the corresponding custom function number is passcode protected. The **CF### Custom Function** prompt is under 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 Function List > M# Function prompt.
- **128 to 143 Enable Custom Function 128 through 143 (128 through 131 for D7412GV4/ D7212GV4) (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.

**NOTICE!**
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.

**NOTICE!**
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.

**NOTICE!**
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 6.2 Schedules (Skeds), page 164*.

**Example 1**
Execute the third function in a keypad menu function list:
- D1255: CDDE
- D1260: C8C7C5

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

**Example 2**
Instant master Arm (CMD 11):
- D1255: A11
- D1260: A11

ℹ **NOTICE!**

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

ℹ **NOTICE!**

The GV4 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.

## 3.12 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.

### 3.12.1 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 *D9412GV4/D7412GV4/D7212GV4 Program Record Sheet* (P/N: F01U214958) 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.

### 3.12.2 Command Authorization

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

| Selection | Description |
|---|---|
| - | 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 *Section 3.12.6 Authority Level Selections, page 102*. |

**Table 3.17** Keypad Programming Choices

**NOTICE!**
Refer to *Section 3.12.6 Authority Level Selections, page 102* 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:** | -, 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]. |
| - | 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.

### Master Arm Instant

| | |
|---|---|
| **Default:** | - (Disabled) |
| **Selection:** | -, 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**

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

### Perimeter Instant

| | |
|---|---|
| **Default:** | - (Disabled) |
| **Selection:** | -, 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 5.2 Point Responses, page 132*) 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**

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

### Perimeter Delay

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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:** | -, 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 3.14.1 Area Relays, page 118*).

### Perimeter Partial

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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.

**NOTICE!**
**Perimeter Partial** ignores the **A# Force Arm/Bypass Max** entry in *Section 3.10 Area Parameters, page 61*.

**NOTICE!**
**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:** | -, E, or P |

| **Function No.** | **Function Name** | **Alternate Keystroke** |
|---|---|---|
| 8 | View Area Stat | (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 # PERIMETER 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:** | -, 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 Point Status

| | |
|---|---|
| **Default:** | E |
| **Selection:** | -, 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:** | -, 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:** | -, 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:** | E |
| **Selection:** | -, 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 Report** is enabled in *Section 3.1 Phone, page 17*.

## 3.12.3 Access Control Functions

### Door Control

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, E, or P |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 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 3.12.6 Authority Level Selections, page 102*). Use this item when programming door control in your function menu.

**Access Control Level**

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, E, or P |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 37 | Access Control Levels | (Menu function only) |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

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.

**Change Display**

| | |
|---|---|
| **Default:** | E |
| **Selection:** | -, 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.

**Change Time/Date**

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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.

**Change Passcode**

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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.

**NOTICE!**
Refer to *Section 3.12.6 Authority Level Selections, page 102* for a detailed description of the functions on the following pages. These parameters determine only if the authority level functions are passcode protected.

**NOTICE!**
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:** | -, 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:** | -, E, or P |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 18 | Delete User | [COMMAND][5][3] |

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

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

### Extend Close

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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:** | -, 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.

### Print Log

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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 Command 7

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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 POINTS > Command 7 / Command 9 section.

### User Command 9

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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 POINTS > Command 7 / Command 9 section.

### Bypass a Point

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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 3.11.1 Keypad (Command Center) Assignment, page 79*.
The control panel ignores alarms and troubles, and does not display point faults when a point is bypassed.

### Unbypass a Point

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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## Force Arm Returnable** or **P## Bypass Returnable**. Points within the scope of the keypad can be unbypassed where the function is entered (refer to *Section 3.11.1 Keypad (Command Center) Assignment, page 79*). The control panel responds to alarms and troubles, and displays point faults when a point is unbypassed.

### Reset Sensors

| | |
|---|---|
| **Default:** | E |
| **Selection:** | -, 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 5.1 Point Index, page 130*. Points within the scope of the keypad where the function is entered reset. Refer to *Section 3.11.1 Keypad (Command Center) Assignment, page 79*.

### Change Relay

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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 D7412GV4 and 1 through 28 in a D7212GV4) that are installed in the system.

### Remote Program

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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:** | -, 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 several sec of no activity at the keypad, the keypad reverts back to the originally programmed area.

### Display Revision

| | |
|---|---|
| **Default:** | E |
| **Selection:** | -, 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:** | -, E, or P |

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

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

**NOTICE!**

The Service Walk Test is available on the D9412GV4 using the Service Menu [9][9][ENT]. The D7412GV4 and D7212GV4 **do not** include the Service Walk Test in the Service Menu. In the D7412GV4 and D7212GV4, the Service Walk Test function must be enabled in the Function List to access the Service Walk Test.

### Default Text

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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:** | -, 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:** | -, 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 Point** function programmed **Yes**.

## 3.12.4 Custom Functions

### C Function 128 [through 143]

| | |
|---|---|
| **Default:** | P |
| **Selection:** | -, 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.

## 3.12.5 Configuration Authority

### Keypad Programming

| | |
|---|---|
| **Default:** | P |
| **Selection:** | - or P |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| N/A | Keypad Programming | Menu function only |

Use this function to make system programming changes. When enabled, only the Service User (Authority Level 15) has authority to access this menu. When disabled (set to -), the programming menu cannot be accessed through the Service User menu.

**NOTICE!**
If at least one area is armed or the control panel is communicating with RPS, you cannot access keypad programming.

**Keypad Programming of the Keypad Programming Option**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **DISABLE KP PROG** option. Press [ENT].
2. The current keypad programming configuration shows (for example, ALLOWED: YES).
3. Press [ENT] to change the configuration. The keypad reads **PRG ALLOWED:** followed by **YES** or **NO**.
4. Press [NEXT] or [PREV] to toggle to **YES** to allow keypad programming or **NO** to disable keypad programming, and then press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**NOTICE!**
You can continue using the current programming session. Keypad programming is disabled once you exit the current session.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Disable Keypad Prog** option.
2. The current keypad programming configuration shows (for example, Keypad Programming Allowed: Yes).
3. Press the **Edit** softkey to change the area’s status.
4. Press the **Yes** or **No** softkey, and then press the **Save** softkey to save the changes.
5. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection has been configured.

**NOTICE!**
You can continue using the current programming session. Keypad programming is disabled once you exit the current session.

## 3.12.6 Authority Level Selections

Use this section to determine which Authority Levels can access keypad functions. If a keypad command is Enabled and not passcode protected, then it does not need to be Enabled by Authority Level. All passcode protected keypad commands need to be authorized by user Authority Level.

| Authority Level | Description |
|---|---|
| - | **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. |

**NOTICE!**
To determine the **L##** default values *Page 103* through *Page 115*, refer to the *User Interface* section in the program record sheet.

### L## Disarm

| | |
|---|---|
| **Default:** | Authority Levels 1-5, 14: Enabled (E)Authority Levels 6-13: Blank (-) |
| **Selection:** | - 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.

**NOTICE!**
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 3.10 Area Parameters, page 61* and **CC# Scope** in *Section 3.11.1 Keypad (Command Center) Assignment, page 79*.

### L## Master Arm Delay

| | |
|---|---|
| **Default:** | Authority Levels 1-5: Enabled (E)Authority Levels 6-15: Blank (-) |
| **Selection:** | - 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## Master Arm Instant

| | |
|---|---|
| **Default:** | Authority Levels 1-2: Enabled (E)Authority Levels 3-15: Blank (-) |
| **Selection:** | - 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 Instant function. Refer to *Section  Master Arm Instant, page 94*.

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.

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

### L## Perimeter Instant

| | |
|---|---|
| **Default:** | Authority Levels 1-4: Enabled (E)Authority Levels 5-15: Blank (-) |
| **Selection:** | - 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## Perimeter Delay

| | |
|---|---|
| **Default:** | Authority Levels 1-4: Enabled (E)Authority Levels 5-15: Blank (-) |
| **Selection:** | - 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:**: | Authority Levels 1-3, 15: Enabled (E)Authority Levels 4-14: Blank (-) |
| **Selection:** | - 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## Perimeter Partial

| | |
|---|---|
| **Default:** | Authority Levels 1-4: Enabled (E)Authority Levels 5-15: Blank (-) |
| **Selection:** | - or E |

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

Partially arms only the area where the keypad is assigned.

**NOTICE!**

This function ignores the **A# Force Arm/Bypass Max** entry in Area Parameters.

**NOTICE!**

**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:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1-3, 15: Enabled (E)Authority Levels 4-14: Blank (-) |
| **Selection:** | - 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 Point Status

| | |
|---|---|
| **Default:** | Authority Levels 1-3, 15: Enabled (E)Authority Levels 4-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - 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.

**NOTICE!**

To Walk Test a Door point connected to a D9210C 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:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - 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.

**NOTICE!**
**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:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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**

The following five functions are used to control the doors from the keypad. These features are not available with the D7212GV4.

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.

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

**L## Door Control**

| | |
|---|---|
| **Default:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - or E |

| **Function No.** | **Function Name** | **Alternate Keystroke** |
|---|---|---|
| 14 | Door Control | [COMMAND][4][6] |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

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.

**NOTICE!**
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.

**NOTICE!**
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:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - or E |

| **Function No.** | **Function Name** | **Alternate Keystroke** |
|---|---|---|
| (None) | Cycle Door | (Menu function only) |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

**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 3.18, Page 108*.

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

### L## Unlock Door

| | |
|---|---|
| **Default:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - or E |

| **Function No.** | **Function Name** | **Alternate Keystroke** |
|---|---|---|
| (None) | Cycle Door | (Menu function only) |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

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 3.18, Page 108*). 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 keypad display.

### L## Secure Door

| | |
|---|---|
| **Default:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - or E |

| **Function No.** | **Function Name** | **Alternate Keystroke** |
|---|---|---|
| (None) | Secure Door | (Menu function only) |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

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 3.18, Page 108*).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 keypad display.

| 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. |

**Table 3.18** L## Secure Door-Door Mode Definitions

### L## Access Control Level

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 37 | Access Control Level | (Menu function only) |
| This feature is not available with the D7212GV4. Keep the default setting. | | |

**NOTICE!**
Changing the Access Control Level in any area affects all users and all doors associated with that level for all areas.

## 3.12.7 General Functions

### L## Change Display

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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## Change Time/Date

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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## Change Passcode

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

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

Change a user passcode.

**L## Add User**

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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.

**NOTICE!**
D9210 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 3.11.1 Keypad (Command Center) Assignment, page 79*.

**L## Del User**

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

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

Delete users.

**L## Extend Close**

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 21 | View Log | (Menu funtion only) |

View all panel-wide events in the control panel’s memory log.

**L## Print Log**

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 22 | Print Event Log | (Menu funtion only) |

Print all panel-wide events from the log to the printer in the area where the user is executing this function.

**NOTICE!**
This item can also be accessed using the Service Menu ([9][9][ENT]).

### L## User Command 7

| | |
|---|---|
| **Default:** | Authority Levels 15: Enabled (E)Authority Levels 1-14: Blank (-) |
| **Selection:** | - 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 POINTS > Command 7 / Command 9 section.

### L## User Command 9

| | |
|---|---|
| **Default:** | Authority Levels 15: Enabled (E)Authority Levels 1-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 24 | User Command 9 | [COMMAND][7] |

This command can be used in Function Menu. Generate the alarm programmed at COMMAND 9 in the POINTS > Command 9 / Command 9 section.

### L## Bypass a Point

| | |
|---|---|
| **Default:** | Authority Levels 1-4, 15: Enabled (E)Authority Levels 5-14: Blank (-) |
| **Selection:** | - or E |

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

Bypass points with this authority level.

### L## Unbypass a Point

| | |
|---|---|
| **Default:** | Authority Levels 1-4, 15: Enabled (E)<br>Authority Levels 5-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1-4, 15: Enabled (E)Authority Levels 5-14: Blank (-) |
| **Selection:** | - or E |

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

Reset sensors with this authority level.

### L## Change Relay

| | |
|---|---|
| **Default:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 28 | Change Relay | [COMMAND][5][4] |

Manually activate or reset a system relay.

**NOTICE!**

Do **not** use the Change 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# Enter Key Relay?**

### L## Remote Program

| | |
|---|---|
| **Default:** | Authority Levels 1-4, 15: Enabled (E)Authority Levels 5-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1-2, 15: Enabled (E)Authority Levels 3-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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:

- 9412GV4 REV ##.##

### L## Service Walk

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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.
- Point source is Unassigned and the Point Index is set to 0.

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.

Points 128 and Point 248 are not accessible by this function. This is normal. These points are used for supervising the Zonex 1 bus (Point 128) and Zonex 2 bus (Point 248).This function allows viewing of extra points. Extra points occur under three conditions: the **P### Point Source** is set to anything other than Unassigned, the **P### Point Index** is set to **0**, and at least two points are installed for the same Point Assignment on different Point Sources.

### L## Default Text

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - or E |

| Function No. | Function Name | Alternate Keystroke |
|---|---|---|
| 35 | Default Text | [COMMAND][5][2] |

Change skeds that can be edited.

**NOTICE!**
Editing of skeds can be restricted by programming **S## Time Edit?** to **No**.

### L## Invisible Walk Test

| | |
|---|---|
| **Default:** | Authority Levels 1, 15: Enabled (E)Authority Levels 2-14: Blank (-) |
| **Selection:** | - 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 Point 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 and 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).

#### L## C Function 128 [through 143]

| | |
|---|---|
| **Default:** | Authority Levels 1: Enabled (E)Authority Levels 2-15: Blank (-) |
| **Selection:** | - 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.

### 3.12.8 Report Levels

#### L## Force Arm

| | |
|---|---|
| **Default:** | Authority Levels 1-6: Enabled (E)Authority Levels 7-15: Blank (-) |
| **Selection:** | - or E |

A user with this authority level can Force Arm.

#### L## Area O/C

| | |
|---|---|
| **Default:** | Authority Levels 1-14: Enabled (E)Authority Level 15: Blank (-) |
| **Selection:** | - 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:** | Blank |
| **Selection:** | - 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 3.10.4 Open/Close Options, page 69*.

#### L## Perimeter O/C

| | |
|---|---|
| **Default:** | Authority Levels 1-14: Enabled (E) Authority Level 15: Blank (-) |
| **Selection:** | - 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 in *Section 3.10.4 Open/Close Options, page 69*.

#### L## Send Duress

| | |
|---|---|
| **Default:** | Authority Levels 1-14: Enabled (E)Authority Level 15: Blank (-) |
| **Selection:** | - 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 in *Section 3.10.4 Open/Close Options, page 69*.)

#### L## Passcode Arm

| | |
|---|---|
| **Default:** | Authority Levels 1-6: Enabled (E) Authority Levels 7-15: Blank (-) |
| **Selection:** | - or E |

Arm an area by entering a passcode and pressing [ENTER].

#### L## Passcode Disarm

| | |
|---|---|
| **Default:** | Authority Levels 1-5, 14: Enabled (E) Authority Levels 6-13, 15: Blank (-) |
| **Selection:** | - or E |

Disarm an area by entering a passcode and pressing [ENTER].

## 3.12.9 Access Control Levels

**L## Security Level**

| | |
|---|---|
| **Default:** | Authority Levels 1-2: Master (M)Authority Levels 3-5: Perimeter (P)Authority Level 6: Disarmed (D)Authority Levels 7-15: Blank (-) |
| **Selection:** | M, P, D, or - |
| 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. |
| - | Users do not have access rights to this area. |

Disarm an area by entering a passcode and pressing [ENTER].

**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:** | Authority Levels 1-5: Disarm (D)Authority Levels 6-15: Blank (-) |
| **Selection:** | I, D, or - |
| 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. |
| - | Users do not have disarm rights in this area. |

**NOTICE!**

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.

**NOTICE!**

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 *Section Access Control Readers Assigned to the Shared Area, page 66*.

**L## Function Level**

| | |
|---|---|
| **Default:** | Authority Level 1: Disarmed (D)Authority Levels 2-15: Blank (-) |
| **Selection:** | M, D, C, or - |
| 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. |
| - | User cannot activate the custom function assigned to the door in this area. |

**NOTICE!**
When a token or card can also disarm an area, the custom function starts **after** the area disarms.

**NOTICE!**
A user does not require **L## Security Level** or **L## Disarm Level** authority to activate a custom function with a token or card.

**NOTICE!**
Tokens or cards that are used to execute Custom Functions must have a passcode assigned to the corresponding User###.

### L## Keyfob Arm/Disarm

| **Default:** | Authority Levels 1-6: Enabled (E)Authority Levels 7-15: Blank (-) |
|---|---|
| **Selection:** | Blank (-) or Enabled (E) |
| Blank (-) | This function is not authorized for the user who is assigned this authority level. |
| Enabled (E) | Enabled (E): This function is authorized for the user who is assigned this authority level. |

Allow a user with this authority level to arm or disarm an area by using their assigned keyfob.

**NOTICE!**
Authority Level 15 is reserved for the Service Passcode (User 0). Since the installer is not allowed a keyfob, authority level 15 shall always be disabled (-).

**NOTICE!**
Duress operation when disarming is not applicable when using Keyfobs.

### L## Remote Firmware Update

| **Default:** | Authority Levels 1-6: Enabled (E)Authority Levels 7-15: Blank (-) |
|---|---|
| **Selection:** | Blank (-) or Enabled (E) |
| Blank (-) | This function is not authorized for the user who is assigned this authority level. |
| Enabled (E) | Enabled (E): This function is authorized for the user who is assigned this authority level. |

When local authorization is required, only a security user with the Remote Firmware Update authority enabled shall be able to authorize the update. By default, Remote Firmware Update authority is only enabled for the Service Passcode (Authority level 15).

### 3.12.10 SIA Duress Passcode Options

**USER INTERFACE>Authority Level>L## Disarm**

**USER INTERFACE>Authority Levels>L## Send Duress**

**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** in *Section 3.9 Miscellaneous, page 59*) 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.

## 3.13 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**.

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.

**NOTICE!**

Failing to program **M## Function** or **M## CC Address 1..#** causes COMMAND DISABLED to appear in the keypad display.

**M## Function**

| | |
|---|---|
| **Default:** | M1 through 15 are functions 1, 2, 29, 11, 15, 16, 17, 18, 19, 25, 26, 9, 10, 8, 21.M16 through M32 are 0. |
| **Selection:** | 0 to 30, 32 to 37, and 128 to 143 (131 on D7412GV4 and D7212GV4) |

Enter the function number indicated in the “#” column of the program record sheet or next to the function in *Section 3.12 User Interface, page 93*.

**NOTICE!**

Function numbers 128 to 143 are custom functions and show the text programmed for **CF ### Text**.

**NOTICE!**
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 #]**

| | |
|---|---|
| **Default:** | M1, M2, M13, M15 are Yes for CC1 through CC16M3 .. M12, M14, M16 .. M32 are No for CC1 through CC16 |
| **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.

## 3.14 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 D9412GV4 can also control 128 (64 for the D7412GV4) 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## Relay Response Type** (refer to *Section  P## Relay Response Type, page 138*) is off-normal or in an alarm condition.
- **Relay Reports:** When relay activity is reported to the receiver (refer to *Section 3.3 Routing, page 23*), 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 Change Relay? function, Relay On/Relay Off skeds, and the Remote Account Manager.

Before programming your relays:

- **Do not** use the CHANGE 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 Enter Key Relay and **P## Relay Response 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 reboots. 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 of reboot:
Alarm Bell
Summary Fire
Area Armed
Fire Bell
Summary Alarm
Silent Arm
Summary Fire Trouble
Watch Mode
Perimeter Fault
Summary Trouble
Reset Sensors
AC Fail
Phone Fail
Summary SupBurg
Communications Fail
Summary SupFire

Relay functions that must be reset manually with Change Relay function (COMMAND 54):
Fail To Close
Duress
Force Armed

### 3.14.1 Area Relays

Each area can be assigned a unique relay number for each of the events listed in this section.

**A# Alarm Bell**

| | |
|---|---|
| **Default:** | A |
| **Selection:** | 0, 1 to 128, A, B, C for D9412GV4 |
| | 0, 1 to 64, A, B, C for D7412GV4 |
| | 0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
**A# Burg Time** and **A# Burg Pattern** 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 0. This feature is required for SIA CP-01 compliance.

**A# Fire Bell**

| | |
|---|---|
| **Default:** | A |
| **Selection:** | 0, 1 to 128, A, B, C for D9412GV4 |
| | 0, 1 to 64, A, B, C for D7412GV4 |
| | 0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
Fire Time and Fire Pattern 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.

**NOTICE!**
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**.

**NOTICE!**
To meet UL 864 requirements, set **A# Fire Bell** to a value other than **0**.

### A# Reset Sensors

| | |
|---|---|
| **Default:** | C |
| **Selection:** | 0, 1 to 128, A, B, C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
The Reset Sensors time converts from the 5 sec default time to the time programmed in **A# Verify Time** (*Section 3.10 Area Parameters, page 61*) when a point programmed for **P## Alarm Verify** (*Section 5.1 Point Index, page 130*) enters an alarm condition.

**NOTICE!**
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.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), set **A# Reset Sensors** to a value other than 0.

### A# Fail to Close

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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** (*Section Perimeter Relay, page 178*) is set to **Yes**, the **A# Fail to Close** prompt becomes A# Perimeter Relay.

**A# Force Armed**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

This relay activates when this area is Force Armed. It remains active until the area disarms or the control panel resets.

**NOTICE!**
If Force Bypassing is required during Perimeter Arming, this relay does not activate.

**A# Watch Mode**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
**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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

Activates when a Duress alarm is generated from a keypad assigned to the specified area.

**NOTICE!**
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# Perimeter Fault

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

This relay activates when a point assigned to the specified area and programmed for **P## Silent Bell** goes into alarm.

**NOTICE!**
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.

## 3.14.2 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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

Activates when the control panel responds to an AC power failure as programmed in **AC Fail Time** in *Section 3.6 Power Supervision, page 50*. This relay automatically resets when AC power restores.

**NOTICE!**
Use this relay to create audible annunciation. Enable the keypad’s trouble sounders for all applications except commercial fire systems.

**Battery Trouble**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
Use this relay to create audible annunciation. Enable the keypad’s trouble sounders for all applications except commercial fire systems.

**Phone Fail**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

Activates when a telephone line failure occurs. A time must be entered in Ph Supv Time (refer to *Section 3.2 Phone Parameters, page 19*) for this relay to activate. This relay resets automatically when restoral of the phone line(s) occurs.

**Comm Fail**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

Activates when a control panel cannot communicate a report after making ten attempts to each routing destination. At the same time, COMM FAIL RG displays at the keypad. This relay automatically resets when a report is sent successfully.

**NOTICE!**
Use this relay to report primary digital report failure to an alternate communication device.

**Log % Full**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

This parameter determines how full the memory log should be before initiating a call to RPS at the central station. This allows the memory log to be copied by RPS before messges can be overwritten. An entry of 0 (zero) disables the LOG THRESHOLD and LOG OVERFLOW events. These events are not put in the log nor reported to the D6500/D6600 or to 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 will be 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 again reached. These events are also sent to the control panel's event log and to the local printer(s) if installed.

**Summary Fire**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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 *Section  Fire Summary Sustain, page 175* for details on alternate operation.

**Summary Alarm**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

**NOTICE!**
This relay does not activate for silent and invisible alarms.

**Summary Fire Trouble**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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 Supervisory Fire**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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 Supervisory Burg**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0, 1 to 128 A, B, or C for D9412GV4<br>0, 1 to 64, A, B, C for D7412GV4<br>0, 1 to 24, A, B, or C for D7212GV4 |

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.

## 3.14.3 Relay/Output Configuration

**Relay/Output Destination**

| | |
|---|---|
| **Default:** | On-Board (For Relays A, B, C)<br>Zonex (For all other relays) |
| **Selection:** | On-Board, Zonex, Octo-output |
| On-Board | Reserved for on-board outputs A, B and C. |
| Zonex | Output is located on a Zonex relay module on Zonex 1 or Zonex 2. |
| Octo-output | Output is located on a relay module on the SDI2 bus. |

# 4 Passcodes, Access Credentials, and User Groups

## 4.1 Passcode or Token Worksheet

These programming items assign:

- a passcode for users 001 to 999,
- areas by authority level, and
- a User Group Window.

### 4.1.1 User Credentials

For the D9412GV4, there are 999 users (399 for D7412GV4 and 99 for D7212GV4) consisting of no more than one passcode, one access credential and one key fob each.

### 4.1.2 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. User ID 0 (zero) is reserved for the service user and can not be assigned an access credential or a keyfob.

**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 3.7, Page 34* 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.

### 4.1.3 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].

**NOTICE!**

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 (D9412GV4 and D7412GV4).

When using the ACCESS CONTROL LEVEL 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.

### 4.1.4 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.

### 4.1.5 Tokens and Cards

All standard users that can be assigned a passcode can also be assigned a token or card by programming the **U### Site Code** and **U### Card Data.**

### 4.1.6 Reporting and Logging

The user ID number used in some event reports can be represented differently to accommodate limitations in technology. Keyfob and access users report as standard users. Refer to the table below for User ID representation in each situation.

| User ID Type | Keypad View Log | RPS View Log | Contact ID | ModemIIIa$^2$ | SDI Bus Printer (D9131A) | User Text (Reporting & Printing) |
|---|---|---|---|---|---|---|
| Service User | 0 | 0 | F00 | 0 | 0 | SERVICE USER |
| Standard User | 1...254<br>255...999 | 1...254<br>255...999 | 1...254<br>255...999 | 1...254<br>255...999 | 1...254<br>Blank | [Configured text] |
| Time Sync | 5001 | 5001 | F01 | 5001 | Blank | AUTO TIME SYNC |
| RPS User | 5002 | 5002 | F02 | 5002/Blank | Blank | BY RPS |
| Automation User | 5003 | 5003 | F03 | 5003/Blank | Blank | BY AUTOMATION |
| Keyswitch | 5004 | 5004 | F04 | 5004 | Blank | BY KEYSWITCH |
| No User Specified | Blank | Blank | 000 | Blank | Blank | Blank |

**NOTICE!**

In reporting systems using ModemIIIa$^2$ reporting 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 *Section Point/ User Flag, page 19*.

**NOTICE!**

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 gives an error tone and prohibits the operation.

User 000 cannot be added or changed by the Add/Change user command (COMMAND 56) except by a user with the Service Passcode.

**U### Passcode**

| | |
|---|---|
| **Default**: | User 001 is 123456, All other user passcodes are Blank. |
| **Selection:** | Three to six digits ( 0 to 9) |

Enter three to six digits to enable a passcode for the master user in this group.

**NOTICE!**

To meet UL 864 requirements (D9412GV4 and D7412GV4), enter at least one Passcode.

**NOTICE!**
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.

**NOTICE!**
The authority to silence a bell is granted to all passcodes with authority level 1 or greater. A user passcode can silence a Fire or Burg bell as long as any authority level of 1 or higher is assigned to the area where the bell can be silenced.

### U### User Group

| | |
|---|---|
| **Default**: | 0 |
| **Selection:** | 0 = no group, 1 to 8 |

Create a group of users whose command authority can be enabled and disabled using an automatic user window. The user group 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.

**NOTICE!**
To enable this user’s passcode at all times, leave **U### User Group** set to default (0).

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 remote programming software (RPS).

### U### Area 1 [through Area #] Auth

| | |
|---|---|
| **Default**: | User 000 is Level 15 for All areas.User 001 is Level 1 for Area 1, 0 for Areas 2-32.All other users are Level 0 for all areas. |
| **Selection:** | 0 to 14 |

Assign an authority level to the user for this area. A setting of 0 means the user has no authority in this area.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), assign an authority level of 1 to 14 to the Passcode to silence bells.

### U### Name

| | |
|---|---|
| **Default:** | USER ### |
| **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.

**NOTICE!**
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 D9412GV4/D7412GV4 and D9210C Access Control Interface Module 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 D9210C door control module. Refer to the *D9210C Installation and Operation Guide* (P/N: F01U215244) for information on these readers.

For more information, refer to the Security Industry Association (SIA) Access Control 26-bit Wiegand Reader Interface Standard.

**U### Site Code**

| | |
|---|---|
| **Default:** | 255 |
| **Selection:** | 0 to 255 |
| This feature is not available with the D7212GV4. Keep the default setting. | |

**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 D9412GV4/ D7412GV4 Control Panels.

**NOTICE!**
**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### Site Code**. Your card data is 51888. Enter it into **U### Card Data**.

*A hexadecimal number can contain all numerals. If the code does not work, try converting the number from hexadecimal to decimal.

**NOTICE!**
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### Card Data**

| | |
|---|---|
| **Default**: | Blank |
| **Selection:** | 00000 = (0) to 65534 or Blank (65535) |
| This feature is not available with the D7212GV4. Keep the default setting. | |

**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### Site Code** before programming this prompt.

**U### Keyfob ID**

| | |
|---|---|
| **Default** | 0 |
| **Selection:** | 0 - 99999999 |

Each user can be assigned a wireless keyfob ID. A Keyfob RFID can be Auto-Learned through the SDI2 bus RF receiver, or it can be entered here. Auto-Learned RFIDs can be edited for Keyfob replacement, or can be set to 0 to disable a users Keyfob. A RFID (Radio Frequency device IDentification number) is a unique number assigned to a wireless device at the factory. It provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting.

**NOTICE!**
Duplicate ID detection must be based on the RFID value stored in configuration memory, not on the number printed on the device.

**NOTICE!**
Keyfobs are not supervised when assigned to a User.

# 5 Points

## 5.1 Point Index

Use the point indexes 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 *D9412GV4/D7412GV4/D7212GV4 Program Record Sheet* (P/N: F01U214958) and RPS contain the default settings and descriptions for point indexes.

**P## Type**

| **Default** | **Refer to the program record sheet** |
|---|---|
| **Section** | 0 to 9, or 11 |
| **P## Type** | Description |
| 0 | **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 *Section  P## Fire Point, page 143*), panic, medical, and police alerts.<br>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. |
| 1 | **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.<br>Perimeter points can be programmed to activate entry delay time. If the point activates entry delay, it can also activate an entry tone.<br>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.<br>Perimeter points programmed for an instant point response, generate an alarm immediately when faulted, even during entry or exit delay. |
| 2 | **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.<br>**Instant Interior Points:** Interior points are usually programmed for an instant alarm (refer to *Section 5.2 Point Responses, page 132*). Points programmed for instant alarms generate alarms immediately, even during entry or exit delay.<br>**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.<br>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.<br>Delayed points can also activate an entry tone at the keypad (refer to the **P## Entry Tone Off** prompt in *Section 5.2 Point Responses, page 132*).<br>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. |

| Default | Refer to the program record sheet |
|---|---|
| 3 | **Interior Follower:** Interior Follower points are armed only by master arming the area. They are not armed when using Perimeter-Arming functions.<br>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.<br>If no entry delay is in effect when a fault occurs for the Interior Follower, it creates an instant alarm.<br>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.<br>**NOTICE!**<br>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. |
| 4* | **Keyswitch Maintained:** Program **P## Point Response** as **1**. Do not connect initiating devices to a Keyswitch point.<br>**Normal:** The area is disarmed.<br>**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.<br>**Open:** When this point changes from normal to open, the area arms. |
| | Program **P## Point Response** as **2**, the point responds as follows:<br>**Normal:** When this point changes from open to normal, the area arms.<br>**Open:** The area is disarmed.<br>**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.<br>Trouble and Restoral Reports are not sent if **Local While Disarmed** is **Yes**.<br>Alarm and Restoral Reports are not sent if **Local While Armed** is **Yes**. |
| 5* | **Keyswitch Momentary:** Used for area arming and disarming. **P## Point Response** must be programmed **1**. Do not connect initiating devices to a Keyswitch point.<br>**N S N:** When this point momentarily changes from normal to shorted to normal, it toggles the armed state of the area.<br>**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.<br>Trouble and Restoral Reports are not sent if **Local Disarmed** is **Yes**. |
| 6* | **Open/Close Point:** Used for point arming and disarming. **P## Point Response** must be programmed **1**. Local bells are silenced through the keypad.<br>**Normal:** The point is armed and sends a Point Closing Report. A Point Closing Report is not sent if Local Armed is **Yes**.<br>**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**.<br>**Short:** The point is disarmed and sends a Point Opening Report. A Point Opening Report is not sent if **Local Armed** is **Yes**. |

| Default | Refer to the program record sheet |
|---|---|
| 7* | **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. **P## Point Response** must be programmed **1**. Local bells are silenced through the keypad. For bell control at the D279, use **P## Type 8**.<br>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.<br>**Normal:** The point is armed and sends a Point Closing Report. Point Closing Report is not sent if **Local Armed** is **Yes**.<br>**Open:** The point is disarmed and sends a Point Opening Report. A Point Opening Report is not sent if **Local Armed** is **Yes**.<br>**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**. |
| 8* | **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 **P## Point Response** as **2**.<br>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.<br>**Normal:** When this point changes from open to normal, the area arms.<br>**Open:** The area is disarmed. The alarm bell silences if an alarm occurred while the area was armed.<br>**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. |
| 9* | **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. |
| 11 | **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. |
| *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. | |

**NOTICE!**

If a point with the type of 11 Aux AC Supervision is bypassed, 24 HOUR PT BYPASSED is shown on the keypads.

## 5.2 Point Responses

### 5.2.1 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 a relay when **P## Relay Response Type** is set to 1 and annunciates a fault at the keypads. To annunciate the off-normal state at a keypad, program **P## Display as Device** as Yes or optionally set **P## BuzzOn Fault** as **1** or **2**. This point response does not generate alarms nor does it activate the Alarm Bell.

**Point Response 8, 9, A, B, and C:** These point responses provide supervisory (24-hour) reporting.

### 5.2.2 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 Trouble** 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 Pattern.

**Supervisory:** A Fire point can send a Fire Supervisory Report and activate the **Summary Fire Sup** and **Summary Fire Trouble**, 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.

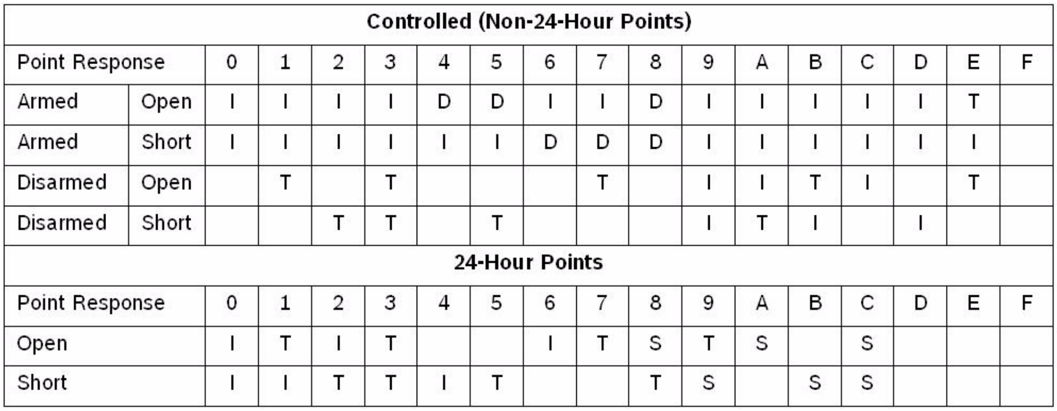
**Reset Sensor:** A fire device that requires resetting can be manually reset using the reset sensor relay for the area to which it is assigned.

**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.

**NOTICE!**
To provide remote annunciation for a restored Fire Supervisory point, use **P## Relay Response Type** set to 1 and connect the corresponding relay to an annunciator.

### P## Point Response

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **Selection:** | 0 - 9, A - 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

S = Supervisory

Blank = Audible or visual response

**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

### 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.

**NOTICE!**
The D1255 alternates between DISARM NOW and the point text of the point that caused the area to enter into entry delay.

If this time expires before disarming, or if the point is configured with an instant response (I), an alarm occurs.

**NOTICE!**
Make entries in 5 sec increments. The programmer does not allow off-increment entries.

With **Passcode Length** set to a non-zero value, entering a valid Passcode during Entry Delay disarms the system as soon as the last digit 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.

**NOTICE!**
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).

**For SIA CP-01 Compliance:**
**P## Entry Delay** must be between 30 sec and 240 sec.

**Tone Off**

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **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.

**WARNING!**
Do not set points to **Yes** 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.

**NOTICE!**
Entry Tone can also be turned off when programming your CC Entry Tone in *Section 3.11 Keypad (Command Center), page 78*, that allows you to manage the tone by keypad.

**NOTICE!**
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:** | Refer to the program record sheet |
| **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. |

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.

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), set this parameter to **No**.

**NOTICE!**
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 Until Restored

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **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.

**NOTICE!**
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.

**NOTICE!**
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:** | Refer to the program record sheet |
| **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.

**NOTICE!**
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.

### P## Invisible Point

| | |
|---|---|
| **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. |

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), 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.

**NOTICE!**
To prevent the keypad alarm tone and the **A# Burg Alarm** bell from sounding, program **P## Silent Bell** as **Yes**.

**NOTICE!**
If a user enters a valid passcode while a bell is ringing for an invisible alarm, the keypad shows ALARM SILENCED.

**P## Buzz On Fault**

| **Default:** | Refer to the program record sheet | |
|---|---|---|
| **Selection:** | 0 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) |
| 0 | 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. |

**NOTICE!**
Points bypassed (by the user, Sked, Swinger Bypass, or RPS) do **not** generate a Buzz On Fault condition at the keypad.

**NOTICE!**
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.

### 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## Relay Response Type

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **Selection:** | 0 to 2 |
| 0 | 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 D9412GV4; 1 to 64 for D7412GV4) 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 (D9412GV4 only). Refer to the address settings on the back of the *D9412GV4/D7412GV4/D7212GV4 Program Record Sheet* (P/N: F01U214958).

**NOTICE!**
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.

**NOTICE!**
Do **not** use the Change 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## Enter Key Relay and **P## Relay Response Type**.

### P## Display as Device

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **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## Display as Device** to cause the keypad to display CHECK DEVICE when a point is off-normal or is acknowledged after going into alarm.

**NOTICE!**
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.

**NOTICE!**
To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), 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.

**NOTICE!**
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.

**P## Local While Armed**

| | |
|---|---|
| **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 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.

**NOTICE!**
To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), 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.

ℹ **NOTICE!**

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## Disable Restorals

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **Selection:** | Yes or No |
| Yes | Enable Restoral Reports from this point. |
| No | Disable Restoral Reports from this point. |

* 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.

ℹ **NOTICE!**

To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), 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## Force Arm Returnable

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **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.

ℹ **NOTICE!**

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## Bypass Returnable

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **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.

ℹ **NOTICE!**

Set this item to No for Interlock points.

**NOTICE!**
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).

**NOTICE!**
For Force Armed points to remain bypassed, ensure that **P## Force Arm Returnable** is set to **No**.

**P## Bypassable**

| **Default:** | Refer to the program record sheet |
|---|---|
| **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 *Section 3.10.4 Open/Close Options, page 69* or by a Sked programmed to arm the area. |

**NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), set this parameter to No.

**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.

**NOTICE!**
**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.

**NOTICE!**
**If the P## Bypassable option is set to Yes**, a point can be bypassed in several ways. Refer to *Table 5.1*.

| **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* |
| *RPS Bypass is sent at the end of the RPS session. | |

**Table 5.1** Bypassing a Point

**NOTICE!**
If the **P## Swinger Bypass 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.

**NOTICE!**
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 Bypass

| **Default:** | Refer to the program record sheet |
|---|---|
| **Selection:** | Yes or No |
| Yes | Enable Swinger Bypass for this point. |
| No | Disable Swinger Bypass for this point. |

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

Use the **P## Swinger Bypass** 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 *Section  Swinger Count, page 177*).
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.

**NOTICE!**
**P## Bypassable** does not need to be programmed as **Yes** for swinger bypass to work.

**NOTICE!**
A Swinger Shunted point returns to the system if **P## Bypass Returnable**? is Yes. If not, return the point to the system through manual unbypass or [COMMAND][0][0]. Refer to **P## Bypass Returnable** in the program entry guide for additional information.

### P## Report Bypass at Occurrence

| **Default:** | Refer to the program record sheet |
|---|---|
| **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 *Section  P## Defer Bypass Report, page 142*.

### P## Defer Bypass Report

| **Default:** | Refer to the program record sheet |
|---|---|
| **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.

**NOTICE!**
When **P## Defer Bypass 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**.

**NOTICE!**
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:** | Refer to the program record sheet |
| **Selection:** | Yes or No |
| Yes | This point is a Cross Point. |
| No | This point is not a Cross Point. |

**NOTICE!**
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 P## Cross Point, page 143* 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 *Section P## Alarm Abort, page 145*) set to **Yes**.

**NOTICE!**
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:** | Refer to the program record sheet |
| **Selection:** | Yes or No |
| Yes | This point is a Fire point. |
| No | This point is not a Fire point. |

ⓘ **NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), 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 Characteristics of a Fire Point *Section 5.2 Point Responses, page 132*.

ⓘ **NOTICE!**
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).

ⓘ **NOTICE!**
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.<br>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 3.10 Area Parameters, page 61*. 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.

ⓘ **NOTICE!**
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. |

ⓘ **NOTICE!**
To meet UL 864 requirements (D9412GV4 and D7412GV4), 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.

**NOTICE!**
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:** | Refer to the program record sheet |
|---|---|
| **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 *Section  CC# Abort Display, page 87*.

**For SIA CP-01 Compliance:**
**P## Alarm Abort** can be set to **Yes** or **No**.

**NOTICE!**
This feature does not apply to Fire Alarms or invisible point alarms.

### P## Wireless Point Supervision Time

| **Default** | Refer to the program record sheet |
|---|---|
| **Selection:** | None, 4 hr, 12 hr, 24 hr, 48 hr, 72 hr |
| None | No wireless point supervision. |
| 4 hr | Send a missing condition after 4 hr of no contact from the wireless device. |
| 12 hr | Send a missing condition after 12 hr of no contact from the wireless device. |
| 24 hr | Send a missing condition after 24 hr of no contact from the wireless device. |
| 48 hr | Send a missing condition after 48 hr of no contact from the wireless device. |
| 72 hr | Send a missing condition after 72 hr of no contact from the wireless device. |

A fire point follows the supervision rules if configured as a point device. Fire points have a fixed supervision interval of 4 hours, regardless of **Wireless Point Supervision Time** setting. If a Fire Point setting is **Yes**, then the **Wireless Point Supervision Time** setting must be set to 4 hours. This is an alternate supervision interval to the global System Supervision Time setting. Refer to *Section  System Supervision Time, page 190*.

## 5.3 Point Assignments

These entries assign point indexes to Points 1 to 127, 129 to 247 for the D9412GV4, Points 1 to 75 for the D7412GV4, Points 1 to 40 for the D7212GV4, 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.

**P### Point Source**

| | |
|---|---|
| **Default:** | On-Board for Points 1 to 8, Wireless for point 9<br>Unassigned for all other points |
| **Selection:** | Unassigned, Zonex, Octo-input, Wireless, On-Board, Door Point |
| Unassigned | Point is not installed. |
| Zonex | Point is installed on a Zonex bus input module. Including Zonex RF point. |
| Octo-input | Point is installed on an SDI2 bus input module. |
| Wireless | Point is installed on an SDI2 bus RF receiver. |
| Onboard | Point is installed on control panel. |
| Door Point | Point is installed on a SDI bus Door Controller. Not selectable here. |

**NOTICE!**
The Door Point option for P## Point Source is not selectable from the Point Assignment menu. To select Door Point option, set the point assignment number in **ACCESS CONTROL > Door, Strke, and Event Profiles > D# Door Point.**

**NOTICE!**
Point number 128 is reserved for supervising Zonex 1.
Point number 248 is reserved for supervising Zonex 2 (D9412GV4).

**P### Point Index**

| | |
|---|---|
| **Default:** | Refer to the program record sheet |
| **Selection:** | 0 to 31 |

This entry selects one of the 31 Point Index codes that define the point's characteristics and determines how the control panel responds to various point conditions.

A setting of **0** 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.

**Keypad Programming of P### Point Index**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **POINT PARAMETERS** option. The **PT NUM 1 - ###** option shows.
2. Enter the point number you wish to configure and press [ENT].
3. The keypad shows the point number and the index number (for example, INDEX: 3).
4. Press [ENT]. An invisible editing cursor is enabled for point index number.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the index number, and then enter the new index number.

**NOTICE!**
The keypad does not accept invalid index numbers.

6. Press [ENT] to save the changes.

When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

Press [ENT] to save the changes

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access Keypad Programming and navigate to the **Point Parameters** option.
2. Press [ENTER]. The **Point Num 1 – 247** (1 – 75 for a D7412GV4) option shows.
3. Enter the point number you wish to configure and press [ENTER]. The keypad reads **Point# Index**, and then the currently configured index number (for example, Point (1) Index: 3).
4. Press the **Edit** softkey to change the point index.
5. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire index number. Use the softkeys and the number buttons on the keypad to enter the new point index number.
6. Press the **Save** softkey to save the changes.

When the keypad reads **Parameter Saved**, your selection has been configured.

**P### Area Assign**

| | |
|---|---|
| **Default:** | 1 |
| **Selection:** | 1 to 32 for D9412GV4<br>1 to 8 for D7412GV4<br>1 to 4 for D7212GV4 |

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.

**NOTICE!**
Use an entry of two or higher. Interior Follower points need a Debounce value of at least three.

**NOTICE!**
Door points assigned to D9210C modules need a Debounce value of at least four (D9412GV4 and D7412GV4).

**NOTICE!**
**P### debounce** does not apply to wireless points.

### P### Relay Codes/Relays

| | |
|---|---|
| **Default:** | Points 1..8 are set to Relay Codes 1..8 respectively<br>All other points are 0. |
| **Selection:** | 0: Disabled<br>1 to 8 |

Use this option to activate a relay when the point is faulted. Refer to *Table 5.2*.

**NOTICE!**
Relays do not activate for Fire Supervisory or Non-Fire Supervisory points.

| **Faults Relay** | | | |
|---|---|---|---|
| **Relay Code** | **D8129 on Zonex Bus 2 for D9412GV4*** | **D8129 on Zonex Bus 2 for D9412GV4*** | **D8129 on Zonex Bus 1 for D7412GV4*** |
| 1 | 73 | 9 | 9 |
| 2 | 74 | 10 | 10 |
| 3 | 75 | 11 | 11 |
| 4 | 76 | 12 | 12 |
| 5 | 77 | 13 | 13 |
| 6 | 78 | 14 | 14 |
| 7 | 79 | 15 | 15 |
| 8 | 80 | 16 | 16 |
| * Address setting = 1 (on), 2 (off), 3 (on), 4 (on) | | | |

**Table 5.2** P## Relay Codes

**NOTICE!**
Do not assign a relay to Invisible points. To avoid activating one of the associated relays, program this prompt as 0.

**NOTICE!**
Two relays can activate when this point enters into alarm if the **P## Relay Response 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 IIIa$^2$ 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.

**P### RFID**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 to 99999999 |

A point RFID can be Auto-Learned through the SDI2 bus RF receiver, or it can be entered here. Auto-Learned RFIDs can be edited for point replacement, or can be set to 0 to disable a RF point. A RFID (Radio Frequency device IDentification number) is a unique number assigned to a wireless device at the factory. It provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting.

## 5.4 Cross Point Parameters

This section discusses the requirements necessary to program Cross Point functions.

**NOTICE!**
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 38) 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 D9412GV4 and ten in the D7412GV4. 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 5.3, Page 151* 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.

| 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 |

**Table 5.3** Cross Point Ranges Within Groups

Refer to *Section 3.3 Routing, page 23* 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 |

The Cross Point Time is the duration of the cross point window or the amount of time the control panel waits for a second point within the same cross point group to fault before generating an Cross Zone Alarm event. If a second point is not faulted within the Cross Point Time, then a Burglar Alarm event is generated. Refer to *Table 5.3, Page 151* for Cross Point Group assignments.

## 5.5 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:** | 0 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.

**NOTICE!**
The point index code used for COMMAND 7 must not be used for any other points on the system.

**NOTICE!**
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**.

### CMD7 Relay

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 to 8 |

This entry selects a relay (73 to 80 for the D9412GV4 or 9 to 16 for the D7412GV4 and D7212GV4) when COMMAND 7 is initiated (refer to the *Section  P### Relay Codes/Relays, page 148* for relay number association).

**NOTICE!**
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 IIIa$^2$ format (if it is a reporting point).

### CMD9 Point Index

| | |
|---|---|
| **Default:** | 31 |
| **Selection:** | 0 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.

**NOTICE!**
The point index code used for COMMAND 7 and COMMAND 9 must not be used for any other points on the system.

**NOTICE!**
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**.

### CMD9 Relay

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 to 8 |

This entry selects a relay (73 to 80 for the D9412GV4 or 9 to 16 for the D7412GV4 and D7212GV4) when COMMAND 9 is initiated (refer to *Section  P### Relay Codes/Relays, page 148* for relay number association).

**NOTICE!**
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 appears at keypads (if the point is programmed as visible) and sent to the D6500 or D6600 when transmitting in Modem IIIa$^2$ format (if it is a reporting point).

# 6 Schedules (Skeds)

## 6.1 Windows

Use this programming module to define the windows for Opening and Closing and User Access.

### 6.1.1 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** i**n 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 at default (00:00) 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 *Figure 6.5, Page 161* through *Figure 6.9, Page 162*).

**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 6.1, Page 154*.

| 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 |

**Table 6.1** Window Selections

**Windows**

**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)<br>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).

**NOTICE!**
Avoid programming the Open Early Begin time before a time that is between another window's Open Window Start and Open Window Stop times.

**NOTICE!**
Do **not** program a window to cross the midnight boundary.

Disabled windows have a beginning time of 00:00. If the entry for this prompt is 00:00, 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 00:00.

**NOTICE!**
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.

**NOTICE!**
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 *Section  W# Open Early Begin, page 155* 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.

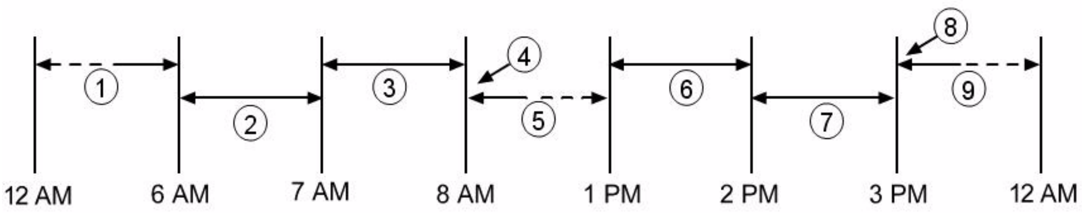


**Figure 6.1** Example Opening Window Timeline (Using Two Opening Windows on the Same Day)

| Callout | Description |
|---|---|
| 1 | Areas disarmed between midnight and 6 AM generate Opening Reports. |
| 2 | Areas disarmed between 6 AM and 7 AM generate Early to Open Reports. |
| 3 | If the area is disarmed between 7 AM and 8 AM regular Opening Reports are generated. If **Disable O/C in Window** is programmed Yes the Opening Report is not sent to the central station. |
| 4 | If the area is not disarmed by 8:01 AM, a **Fail to Open** Event is generated if **Fail to Open** is programmed Yes in Opening and Closing Options. |
| 5 | If the user disarms the area between 8:01 AM and 12:59, PM a Late to Open Event is generated. |
| 6 | Areas that are disarmed between 1 PM and 2 PM generate Early to Open Reports. |
| 7 | If the area is disarmed between 2 PM and 3 PM regular Opening Reports are generated. If Disable O/C in Window is programmed Yes, the Opening Report is not transmitted to the central station. |
| 8 | If the area is not disarmed by 3:01 PM, a Fail to Open Event is generated if Fail to Open is programmed Yes in Opening and Closing Options. |
| 9 | If the user disarms the area between 3:01 PM and 11:59 PM, a Late to Open Event is generated. |

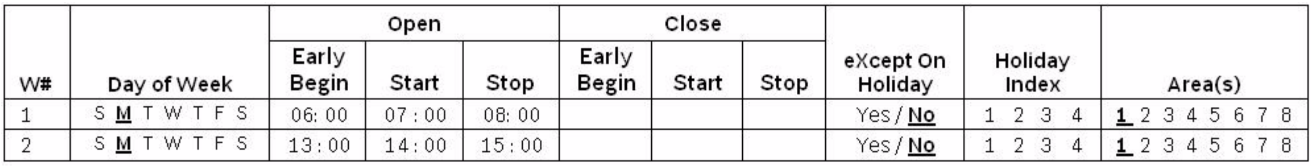
**NOTICE!**

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 *Section W# Open Early Begin, page 155* for additional explanations of report features.

**NOTICE!**

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.

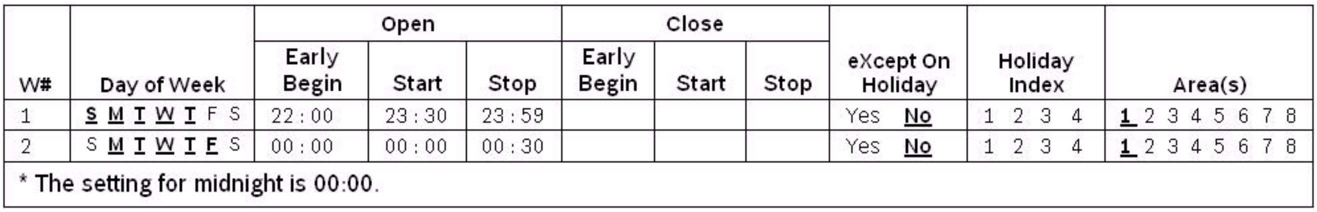


| W# | Day of Week | Open | | | Close | | | eXcept On Holiday | Holiday Index | Area(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Early Begin | Start | Stop | Early Begin | Start | Stop | | | |
| 1 | S [✓ M] T W T F S | 06: 00 | 07 : 00 | 08: 00 | | | | Yes / [✓ No] | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 2 | S [✓ M] T W T F S | 13 : 00 | 14 : 00 | 15 : 00 | | | | Yes / [✓ No] | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |

**Figure 6.2** Programming for Two Same Day Opening Windows (refer to *Figure 6.1, Page 157*)

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 Figure 6.3.



| 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 | [✓ 1] 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 | [✓ 1] 2 3 4 5 6 7 8 |

* The setting for midnight is 00:00.

**Figure 6.3** Programming to Link Two Days over Midnight*

### W# Close Early Begin

| | |
|---|---|
| **Default:** | 00:00 |
| **Selection:** | HH:MM (hours and minutes)<br>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).

**NOTICE!**
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 beginning time of 00:00. If the entry for this prompt is 00:00, 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 00:00.
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

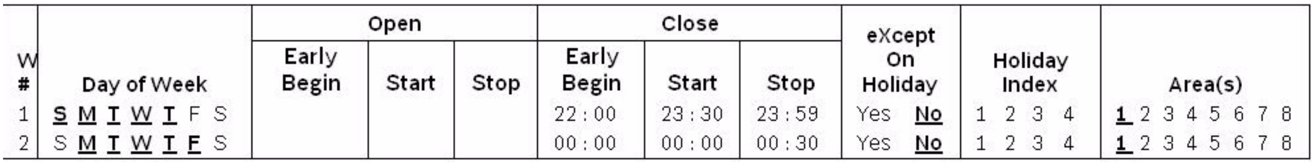
| | |
|---|---|
| **Default:** | 00:00 |
| **Selection:** | HH:MM (hours and minutes) |

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 *Section  W# Close Early Begin, page 158* 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 Start 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 *Section  W# Close Early Begin, page 158* 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 *Figure 6.5, Page 161*.



| 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 | **1** 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 | **1** 2 3 4 5 6 7 8 |

**Figure 6.4** Programming Example: Linking Two Closing Windows over Midnight

### W# Xept Holiday

| | |
|---|---|
| **Default**: | No |
| **Selection:** | Yes or No |
| Yes | Do not activate this window on holidays.<br>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.<br>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 6.3 Holiday Indexes, page 173*.

### 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. |

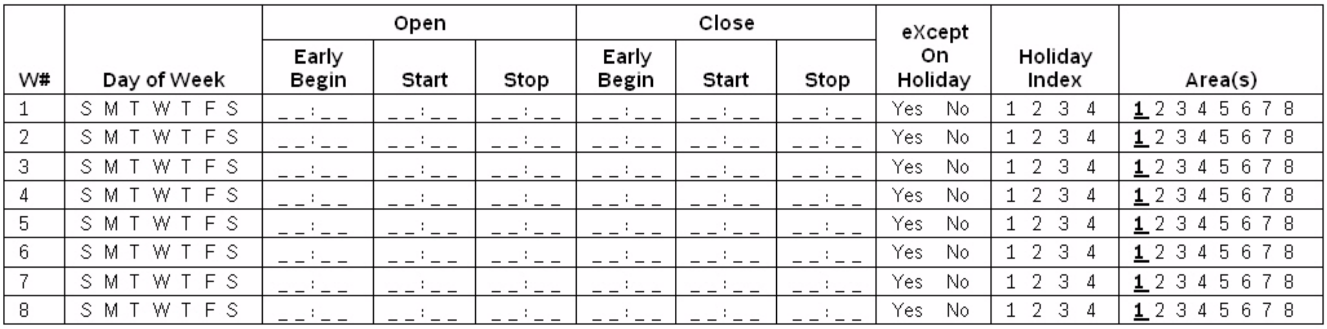
### W# Holiday 4

| | |
|---|---|
| **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# Holiday Area 1 [through 8]

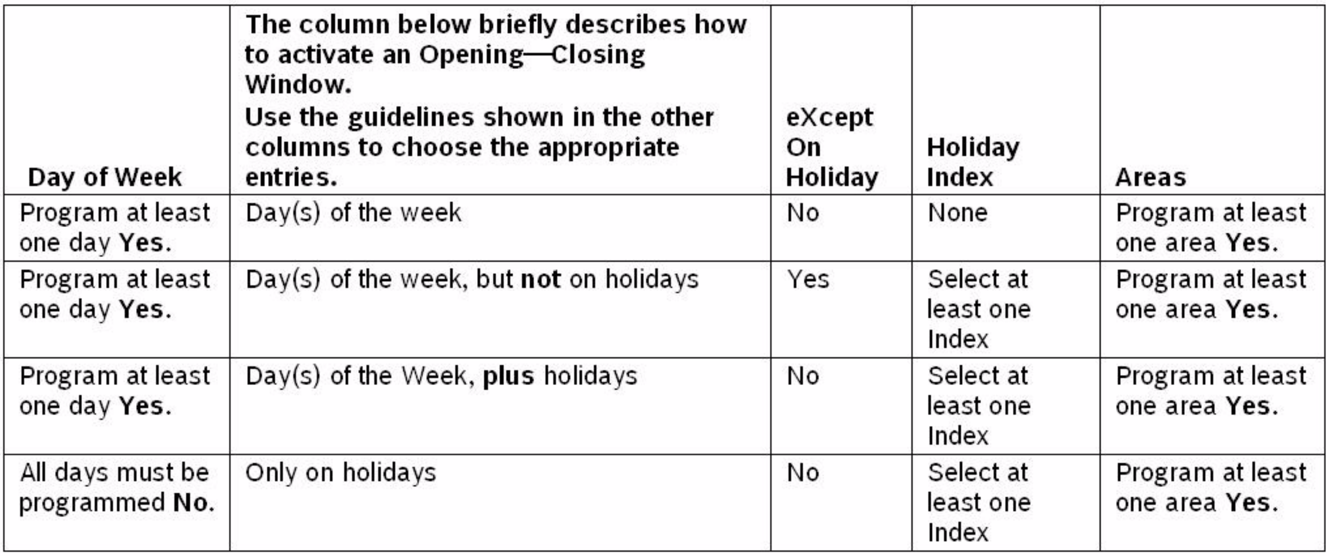
| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |
| Yes | Activate the window in the area number (#) specified. |
| No | Disable the window in the area number (#) specified. |

Eight separate program items determine whether a particular window activates in each of the eight areas of the control panel.



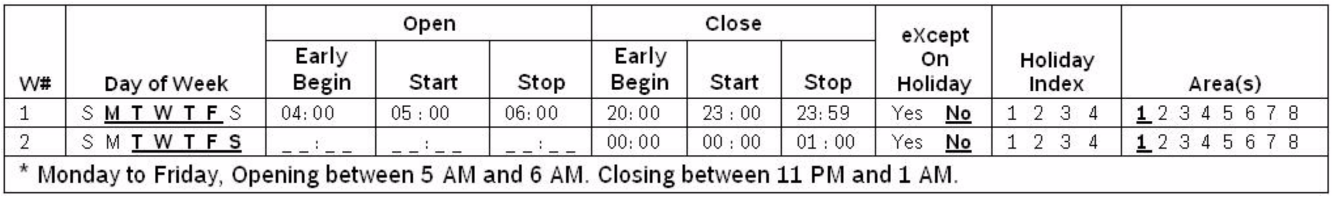
| W# | Day of Week | Open | | | Close | | | eXcept On Holiday | Holiday Index | Area(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Early Begin | Start | Stop | Early Begin | Start | Stop | | | |
| 1 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 2 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 3 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 4 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 5 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 6 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 7 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 8 | S M T W T F S | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | Yes No | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |

**Figure 6.5** Opening and Closing Windows Worksheet



| **Day of Week** | **The column below briefly describes how to activate an Opening—Closing Window.**<br>**Use the guidelines shown in the other columns to choose the appropriate entries.** | **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.** |

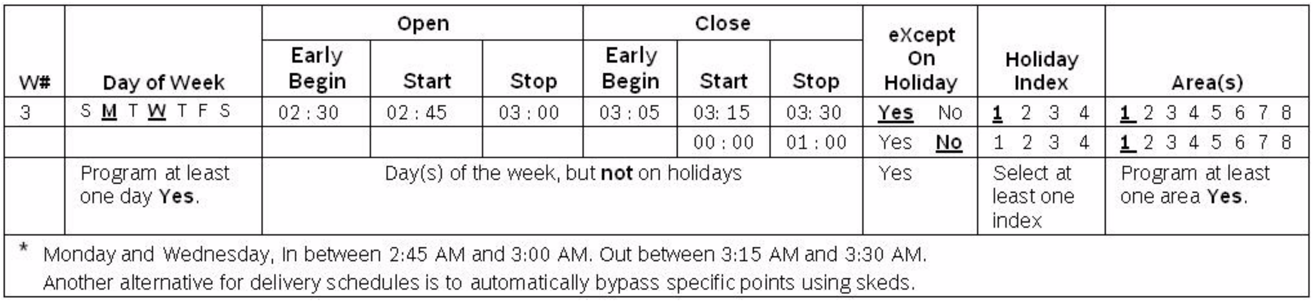
**Figure 6.6** Opening and Closing Windows



| 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 | 04:00 | 05 : 00 | 06:00 | 20:00 | 23 : 00 | 23:59 | Yes [✓ No] | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |
| 2 | S M [✓ T] [✓ W] [✓ T] [✓ F] [✓ S] | _ _ : _ _ | _ _ : _ _ | _ _ : _ _ | 00:00 | 00 : 00 | 01 : 00 | Yes [✓ No] | 1 2 3 4 | [✓ 1] 2 3 4 5 6 7 8 |

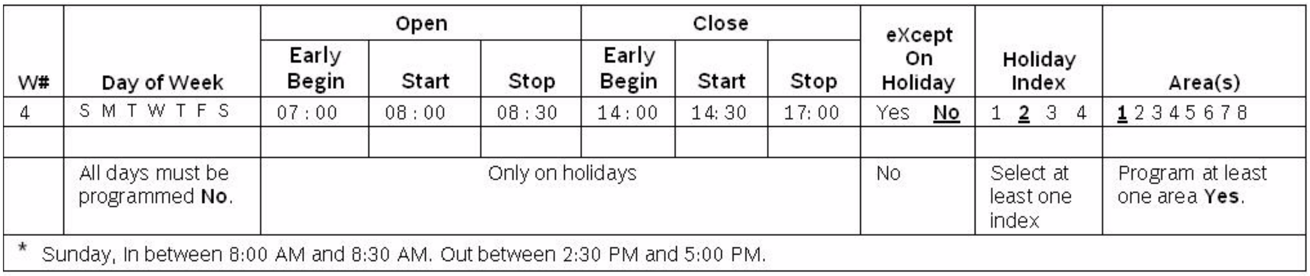
* Monday to Friday, Opening between 5 AM and 6 AM. Closing between 11 PM and 1 AM.

**Figure 6.7** Normal Store Hours*



| W# | Day of Week | Open | | | Close | | | eXcept On Holiday | Holiday Index | Area(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Early Begin | Start | Stop | Early Begin | Start | Stop | | | |
| 3 | S **M** T **W** T F S | 02 : 30 | 02 : 45 | 03 : 00 | 03 : 05 | 03: 15 | 03: 30 | **Yes** No | **1** 2 3 4 | **1** 2 3 4 5 6 7 8 |
| | | | | | | 00 : 00 | 01 : 00 | Yes **No** | 1 2 3 4 | **1** 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.<br>Another alternative for delivery schedules is to automatically bypass specific points using skeds. | | | | | | | | | | |

**Figure 6.8** Delivery 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 **No** | 1 **2** 3 4 | **1** 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. | | | | | | | | | | |

**Figure 6.9** Monthly Auditor’s Schedule*

## 6.1.2 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 *Section U### User Group, page 127* 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.

**NOTICE!**

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 Window

### UW# User Group

| | |
|---|---|
| Default: | 1 |
| **Selection:** | 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.

**NOTICE!**

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.

**NOTICE!**
Refer to *Section  W# Sunday, page 154* 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 Time**

| | |
|---|---|
| **Default:** | 00:00 |
| **Selection:** | HH:MM (hours and minutes) |

**NOTICE!**
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 Time**

| | |
|---|---|
| **Default:** | 00:00 |
| **Selection:** | HH:MM (hours and minutes) |

**NOTICE!**
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, set the time to the default (00:00).
Do not program a single window to cross the midnight boundary. The window stop time must be later than the window start time.

### 6.1.3 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 6.3 Holiday Indexes, page 173* 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 *Section  W# Xept Holiday, page 160*W# Xept Holiday prompt 115.

**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. |

Determine if the window is disabled on holidays, or is active only on holidays. Use the instructions provided in *Section  W# Xept Holiday, page 160*.

## 6.2 Schedules (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 *D9412GV4/D7412GV4/D7212GV4 Program Record Sheet* (P/N: F01U214958), and they are explained in detail following the **S## Function Code** prompt 119.
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 *Section  S## Xept Holiday, page 172*).

### Sked Number

#### 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

RPS 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 #] 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, program the sked for date, day of week, time, or holiday.

| **Default:** | | 0 | | |
|---|---|---|---|---|
| **Selection:** | | 0 = Not In Use, 1 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# Force Arm Bypass Max** setting. | **S## Area 1[through #]**<br>**Default: No**<br>Selections: Yes or No<br>Enable the sked to arm the areas indicated with **Yes**. | **Yes**<br>**No** | Arm Area #.<br>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. | **S## Area 1[through #]**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable the sked to disarm the areas indicated with **Yes**. | **Yes**<br>**No** | Disarm Area #.<br>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. | **S## Point Number**<br>**Default: Blank**<br>**Selections: Blank, 1 to 127, 129 to 247 for D9412GV4, 1 to 75 for D7412GV4, 1 to 40 for D7212GV4**<br>Enter the number of the point the sked bypasses. | **Blank (0)**<br>**1 to 127, 129 to 247** | No point is bypassed<br>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. | **S## Point Number**<br>**Default: Blank**<br>**Selections: Blank, 1 to 127, 129 to 247 for D9412GV4, 1 to 75 for D7412GV4, 1 to 40 for D7212GV4**<br>Enter the number of the point the sked unbypasses. | **Blank (0)**<br>**1 to 127, 129 to 247** | No point is unbypassed.<br>Point to unbypass. |
| 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. | **S## Area 1[through #]**<br>**Default: No**<br>**Selection: Yes or No**<br>Select Yes to unbypass all points in the areas indicated. | **Yes**<br>**No** | Unbypass all points in Area #.<br>Do **not** unbypass all points in Area #. |
| 6 | **Relay On:** This function emulates the Change 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. | **S## Relay Number**<br>**Default: Blank**<br>**Selections: Blank, 1 to 128 for D9412GV4, 1 to 64 for D7412GV4, 1 to 24 for D7212GV4**<br>Enter the number of the relay the sked activates | **Blank**<br>**1 to 128** | No relay is activated.<br>Relay to activate. |
| 7 | **Relay Off:** This function emulates the Change 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. | **S## Relay Number**<br>**Default: Blank**<br>**Selections: Blank, 1 to 128 for D9412GV4, 1 to 64 for D7412GV4, 1 to 24 for D7212GV4**<br>Enter the number of the relay that turns the sked off. | **Blank**<br>**1 to 128** | No relay is turned off.<br>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.<br>No other parameters require input for this option. | | | |

| | | | | |
|---|---|---|---|---|
| 9 | **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 Section 2.3.8 Communication Attempts 20.<br>If **Expand Test Report** in Phone parameters is programmed as **Yes**, the Test Report also includes all off-normal states for events listed in Test Reports (refer to *Section Table 3.9 Test Reports, page 36*) and some events listed in Diagnostic Reports (refer to the footnotes with *Table 3.10, Page 37*)<br>The Test Report can be deferred for up to 24 hours if any other report was sent since the last Test Report. To defer the Test Report, program **S## Defer Test**.<br>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 Report**.<br>**Note:**<br>To meet UL 864 requirements (D9412GV4 and D7412GV4), use the Sked function to meet the daily **Test Report** requirement. | **S## Defer Test**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable sked to defer the Test Report | **Yes**<br>**No** | Defer the Test Report.<br>Send the Test Report on schedule. |
| | | **S## Hourly Report**<br>**Default: No**<br>**Selection: Yes or No**<br>Select Yes to send the Test Report every hour. | **Yes**<br>**No** | Send the Test Report every hour.<br>Send the Test Report only as scheduled. |
| 10 | **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.<br>The Status Report can be deferred for up to 24 hours if any other report was sent since the last Status Report. To defer the Status Report, program **S## Defer Status**. | **S## Defer Status**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable sked to defer the Status Report. | **Yes**<br>**No** | Defer the Status Report.<br>Send the Status Report on schedule. |

| | | | | |
|---|---|---|---|---|
| 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. | **S## Cmd Center**<br>**Default: Blank (0)**<br>**Selections: Blank (0), 1 to 8**<br>Identify the specific keypad (CC #) where the Custom Function is entered. Only one keypad can be assigned for this sked function.<br>**S## Custom Func**<br>**Default: Blank (0)**<br>**Selections: Blank (0), 128 to 143 for D9412GV4, 128 to 131 for D7412GV4 and D7212GV4**<br>Enter the custom function this sked executes. | **Blank (0)**<br>**1 to 8**<br>**Blank (0)**<br>**128 to 143** | No keypad is specified for Custom Function activation.<br>Command center (keypad) address specified for Custom Function activation.<br>No Custom Function is activated. Custom Function to activate. |
| 12 | **Contact RPS:** This function attempts to contact an Unattended RPS at the configured time. The control panel's account in RPS controls the operations performed upon successful contact. | | | |

**CAUTION!**
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.

**NOTICE!**
Ensure that the Custom Function being executed or any of the commands nested inside the Custom Function are not passcode protected.

**NOTICE!**
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:

– For a D1255 keypad type, program "C","C"at the beginning of the Custom Function Key Strokes entry. This aborts the user's function and allows the sked to execute.
– Program the sked to execute at an address (Command Center) with no keypad physically attached to it. The CC # must be assigned to an area and have the appropriate scope programmed.

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 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.<br>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. | | | |
| 15 | **Sound Watch Tone at Command Center (Keypad):** This function sounds the Watch Tone at the keypad address programmed in Parameter 1. The Watch Tone sounds at all keypads with the address programmed. Press [ESC] to silence the tone.<br>Sound Watch Tone defines the keypad address where the Watch Tone sounds. Enter the specific address at the S## Cmd Center prompt. | **S## Cmd Center 1 [through 16]**<br>**Default: Blank**<br>**Selections: Yes or No**<br>Enable the sked to beep the keypad programmed **Yes**. | **Yes**<br>**No** | Watch tone sounds at this keypad.<br>Watch tone does not sound at this keypad. |
| 16 | **Access Control Level On:** (D9412GV4 and D7412GV4) This function emulates the ACCESS CMD LEVEL command that determines whether a user's token or card level is ENABLED?, allowing access granted rights. This affects all doors that this user is assigned to with this specific authority level. | **S## Access Ctl Level #**<br>**Default: No**<br>**Selection: Yes or No**<br>Activate a sked, which enables the Access Level(s) 1 through 14 with Yes. | **Yes**<br>**No** | Enable Access Control for indicated authority levels.<br>Do not enable Access Control for indicated authority levels. |

**NOTICE!**

The D9412GV4 supports eight doors; the D7412GV4 supports two doors.

**NOTICE!**

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:** | | 0 | | |
| **Selection:** | | 0 to 24, 28, 29 | | |
| 17 | **Access Control Level Off:** (D9412GV4 and D7412GV4) This function emulates the ACCESS CMD LEVEL command that determines whether a user's token or card level is disabled. This function allows access to be turned off for the levels programmed. | **S## Access Ctl Level #**<br>**Default: No**<br>**Selections: Yes or No**<br>Enables the sked to turn off access for Levels 1 through 14. | **Yes**<br>**No** | Turn off access for indicated authority levels.<br>Do not turn off access for indicated authority levels. |
| 18 | **Unlock Door:** (D9412GV4 and D7412GV4) This function emulates the UNLOCK? 12345678 keypad function for unlocking a door. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable the sked to unlock the doors programmed **Yes**. | **Yes**<br>**No** | Unlock Door #.<br>Do not unlock Door #. |

| | | | |
|---|---|---|---|
| 19 **Secure Door:** (D9412GV4 and D7412GV4) This function emulates the SECURE? 12345678 keypad function for securing a door. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable the sked to unlock the doors programmed **Yes** to the secured state. | **Yes**<br>**No** | Secure Door #.<br>Do not secure Door #. |
| 20 **Lock Door:** (D9412GV4 and D7412GV4) This function returns an unlocked (Function 18) or secured (Function 19) door to a normal locked door state. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>Enable the sked to lock the doors programmed as **Yes** and return them to the normal Door Mode. | **Yes**<br>**No** | Lock Door #.<br>Do not lock Door #. |
| 21 **Access Authority Events On:** (D9412GV4 and D7412GV4) 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 #. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>This parameter enables the sending of Access Granted Events for Door #. | **Yes**<br>**No** | Enable the sending of Access Granted Events for Door #.<br>Do not enable the sending of Access Granted Events for Door #. |
| 22 **Access Authority Events Off:** (D9412GV4 and D7412GV4) 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 #. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>This parameter disables the sending of Access Granted Events for Door #. | **Yes**<br>**No** | Disable the sending of Access Granted Events for Door #.<br>Do not disable the sending of Access Granted Events for Door #. |
| 23 **No Entry Events On:** (D9412GV4 and D7412GV4) The control panel can log No Entry Events when an invalid token is detected for a specific door. No Entry Events include No Entry-Secured, No Entry-Interlock, No Entry-Unknown ID, and No Entry-Level. These events can be directed to print at a local printer or send a report remotely through phone routing. This sked enables No Entry Events to be reported for Door #. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>This parameter enables the sending of No Entry Events for Door #. | **Yes**<br>**No** | Enable the sending of No Entry Events for Door #.<br>Do not enable the sending of No Entry Events for Door #. |

| | | | | |
|---|---|---|---|---|
| 24 | **No Entry Events Off:** (D9412GV4 and D7412GV4) The control panel can log No Entry Events when an invalid token is detected for a specific door. No Entry Events include No Entry-Secured, No Entry-Interlock, No Entry-Unknown ID, and No Entry-Level. These events can be directed to print at a local printer or send a report remotely through phone routing. This sked disables No Entry Events to be reported for Door #. | **S## Door 1 [through 8]**<br>**Default: No**<br>**Selection: Yes or No**<br>This parameter enables the sending of No Entry Events for Door #. | **Yes**<br>**No** | Enable the reporting of No Entry Events for Door #.<br>Do not enable the reporting of No Entry Events for Door #. |
| 28 | **Expanded Off-Normal Test Report:** To generate this event, one or more points must be in an off-normal state at the time the sked executes. In addition, any system trouble that is active also generates an Expanded Off-Normal Test Report. Expanded Off-Normal Test Reports include the Off Normal Test Report Event as well as the supplementary event at the time the report is generated.<br>The Event Log shows only a Test Report Event.<br>If none of these conditions exists at the time the sked executes, only a Sked Executed Event is generated and the Off-Normal Test Report is not sent. | | | |
| 29 | **Non-Expanded Off-Normal Test Report:** Non-Expanded Off-Normal Test Report Events are only sent when any point is in the off-normal state from any area, but only sends the Off Normal Test Report Event. Any system trouble that is active also generates a Non-Expanded Off-Normal Test Report.<br>The Event Log only shows a Test Report Event.<br>If none of these conditions exist at the time the sked executes, only a Sked Executed Event is generated and the Non-Expanded Off-Normal Test Report is not sent. | | | |

**Table 6.2**

**NOTICE!**

To meet UL 864 daily Test Report requirements (when using two phone lines) (D9412GV4 and D7412GV4), you must still use Sked Function Code 9, Test Report and program it to occur on a daily basis as per AHJ requirements.

### 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 their time set to **Disabled**; however, to ensure that a sked is fully disabled, enter [COMMAND][5][2] (Change Skeds function) and select DISABLE?

### S## Date

| | |
|---|---|
| **Default:** | __/__ |
| **Selection:** | MM/DD (month and date) |

Enter the date that the sked executes.

Disabled skeds have their date set to **Disabled**. If you receive from the control panel and the entry for this prompt is **Disabled**, but dates were programmed before, the sked can be disabled from the keypad using the Change Skeds function.

### 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.

**NOTICE!**

To meet UL 864 requirements for Central Station and Remote Station applications (D9412GV4 and D7412GV4), 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## Wedsday**

| | |
|---|---|
| **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 #**

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |

| | |
|---|---|
| Yes | Use Holiday Index 1 with this sked. |
| No | Do not use Holiday Index 1 with this sked. |

## 6.3 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.

# 7 AUXPARM

## 7.1 Automation

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.

**NOTICE!**
The SIM can be a D9133, DX4010V2, 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.

### 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) at address 80 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.

**NOTICE!**
Trouble SDI 80 Reports are always sent using the account number for Area 1.

### Automation Device

| **Default** | None |
|---|---|
| **Selection:** | SDI Address 80, SDI2 Address 1, SDI2 Address 2 |
| None | Disable Automation |
| SDI Address 80 | Enables the automation address (SDI Address 80) for the DX4010V2 or DX4010V2 Serial Interface Module, or DX4020 Network Interface Module. |
| SDI2 Address 1 | Enables automation and supervision using a B420 Ethernet Communication Module at address 1 on the SDI2 bus. |
| SDI2 Address 2 | Enables automation and supervision using a B420 Ethernet Communication Module at address 2 on the SDI2 bus. |

### Status Rate

**NOTICE!**
If an SDI2 communication device is allocated for automation communication, then it cannot be used for central station nor RPS communication.

| **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. |

**NOTICE!**
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.

## 7.2 Miscellaneous

### Fire Summary Sustain

| **Default** | Yes |
|---|---|
| **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 3.14.2 Panel-Wide Relays, page 121*.

### Fire Supervision Restoral Type

| **Default** | 2 |
|---|---|
| **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.

**NOTICE!**
The Fire Supervision Restore Event is part of Fire Events in Routing. If Fire Supervision Restore Events are needed, simply enable them in Routing.

### Early Ambush Timer

| | |
|---|---|
| **Default** | 10 min |
| **Selection:** | 5 to 30 minutes |

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 *Section  Early Ambush, page 76*) 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.

### Fire Trouble Resound

| | |
|---|---|
| **Default** | 1 |
| **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. |

### 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.

**NOTICE!**
This feature does not apply to Fire Alarms or invisible point alarms.

**For SIA CP-01 Compliance:**
**Abort Window** is a required parameter.

**NOTICE!**
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 *Section P## Entry Delay, page 134*.
**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 | Disabled; 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** | 2 |
|---|---|
| **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 Bypass 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 Bypass** can be **Yes** or **No**. If **P## Swinger Bypass** is **Yes**, **Swinger Count** must be 1 or 2.

**Remote Warning**

| **Default** | No |
|---|---|
| **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 keyfob. |
| 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 keyfob. |

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**.

### Crystal Time Adjust

| **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.

### Daylight Saving Time

| **Default** | US Calendar |
|---|---|
| **Selection:** | Disabled or US Calendar |
| Disabled | The control panel clock is not adjusted for daylight saving time. |
| US Calendar | The control panel clock is adjusted to the US start/end dates for daylight saving. |

# 8 SDI2 Modules

This section discusses programming for the modules that connect to the GV4 Series Control Panel using the SDI2 bus.

Many devices on the SDI2 bus have a tamper input that you can optionally use to monitor the device’s enclosure cover or other tamper switch. This prompt has the same options and purpose for all indicated SDI2 devices.

### Enclosure Tamper

| **Default**: | No |
|---|---|
| **Selection:** | Yes or No |
| Yes | The control panel will monitor the tamper status of an SDI2 device and report its state changes accordingly. |
| No | The control panel will ignore any tamper state changes being sent by an SDI2 device to the panel. |

## 8.1 B208 Octo-input Module

The B208 Octo-input module is a device that attaches to the SDI2 bus of the GV4 Series Control Panel. It provides 8 independently monitored control loops.

| **D9412GV4** | **D7412GV4** | **D7212GV4** |
|---|---|---|
| 24 | 7* | 3* |
| * For the D7412GV4, only 5 inputs are available on the Octo-input at address 7 and for the D7212GV4, only 2 inputs are available on the Octo-input at address 3. | | |

**Table 8.1** B208 Module Capacities Per Control Panel

RPS supports the configuration of the enclosure tamper on each of the Octo-input modules. Refer to *Section  Enclosure Tamper, page 179*.

## 8.2 B308 Octo-output Module

The B308 Octo-output is a device that attaches to the SDI2 bus of the GV4 Series Control Panel. It provides 8 independently controlled outputs similar in function to those provided by the Zonex output modules.

| **D9412GV4** | **D7412GV4** | **D7212GV4** |
|---|---|---|
| 12 | 6* | 2* |
| * For the D7412GV4, only 4 relays are available on the Octo-output at address 6 and for the D7212GV4 only 4 relays are available on the Octo-output at address 2. | | |

**Table 8.2** B308 Module Capacities Per Control Panel

RPS supports the configuration of the enclosure tamper on each of the Octo-output modules. Refer to *Section  Enclosure Tamper, page 179*.

## 8.3 B420 Ethernet Communication Module

The B420 Ethernet Communication Module is used to connect to the control panel over an Ethernet network. Typical uses include PC front-end (automation) software packages, network RPS connection for off-site programming, diagnostic troubleshooting, D6600 NetCom Central Station Receiver (CSR) reporting, and history retrieval. Module bus supervision is enforced when the SDI2 communication module is used in a central station reporting route.

| **D9412GV4** | **D7412GV4** | **D7212GV4** |
|---|---|---|
| 2 | 2 | 2 |

**Table 8.3** B420 Module Capacities Per Control Panel

You can use one or both communication modules for central station reporting or RPS communications. Optionally, you can use one of the B420 modules for communication with automation software. While in this mode, you cannot use the module to communicate with RPS nor with the central station.
RPS supports the configuration of the enclosure tamper on each of the Network Interface Modules. Refer to *Section  Enclosure Tamper, page 179*.

### DHCP/AutoIP Enable

| | |
|---|---|
| **Default:** | Yes |
| **Selection:** | Yes or No |

DHCP is an auto configuration protocol that allows a computer to be automatically configured, which eliminates the need for interaction by a network administrator. DHCP also provides a central database that tracks computers that connect to the network, which prevents two computers from accidentally being configured with the same IP address.
AutoIP enables dynamic IP addresses to be assigned to a device when the device is started up. Whereas DHCP requires a DHCP server, AutoIP does not require a server when selecting an IP address. A host configured with AutoIP receives an IP address of 169.254.xxx.xxx.

**Keypad Programming of DHCP Enable**
**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **MODULE PARAM** option to enter it.
4. Press [ENT] at the **DHCP ENABLE** option. The keypad shows YES or NO.
5. To change the setting, press [EDIT] and then press the button for the desired option.
6. Press [Save] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **Module Parameters** option to enter it.
4. Press [ENTER] at the **DHCP Enable** option. The keypad shows Yes or No.
5. To change the setting, press **Edit** softkey and then press the softkey for the desired option.
6. Press the **Save** softkey to save the changes.

### IPv4 Address

| | |
|---|---|
| **Default:** | 0.0.0.0 |
| **Selection:** | 0.0.0.0 to 255.255.255.255 |

A Domain Name Server (DNS) converts internet domain names or hostnames to their corresponding IP addresses. When this is defined through the DHCP service, leave the default value.

**Keypad Programming of IPv4 Address**
**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **ADDRESS PARAM** option to enter it.

4. Press [ENT] at the **IP ADDRESS** option. The currently configured IP address shows. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad does not accept invalid byte numbers.

6. Repeat *Step 5* to enter the correct numbers for each byte.
7. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **Address Parameters** option to enter it.
4. Press [ENTER] at the **IP Address** option. The current configured IP address shows.
5. To change the setting, press the **Edit** softkey.
6. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire IP address. Use the softkeys and the number buttons on the keypad to enter the new IP address.

**NOTICE!**
The keypad does not accept invalid byte numbers.

7. Press the **Save** softkey to save the changes.

### IPv4 Subnet Mask

| | |
|---|---|
| **Default:** | 255.255.255.0 |
| **Selection:** | 0.0.0.0 to 255.255.255.255 |

This defines the sub-network class. When this is defined through the DHCP service, leave the default value.

### Keypad Programming of IPv4 Subnet Mask

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **ADDRESS PARAM** option to enter it.
4. Press [ENT] at the **SUBNET MASK** option. The currently configured subnet mask address shows. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad does not accept invalid byte numbers.

6. Repeat *Step 5* to enter the correct numbers for each byte.
7. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **Address Parameters** option to enter it.
4. Press [ENTER] at the **Subnet Mask** option. The current configured subnet mask shows.
5. To change the setting, press the **Edit** softkey.
6. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire IP address. Use the softkeys and the number buttons on the keypad to enter the new IP address.

**NOTICE!**
The keypad does not accept invalid byte numbers.

7. Press the **Save** softkey to save the changes.

### IPv4 Default Gateway

| | |
|---|---|
| **Default:** | 0.0.0.0 |
| **Selection:** | 0.0.0.0 to 255.255.255.255 |

This defines the address of the Internet or Intranet gateway. When this is defined through the DHCP service, leave the default value.

### Keypad Programming of IPv4 Default Gateway

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **ADDRESS PARAM** option to enter it.
4. Press [ENT] at the **DEFAULT GATEWAY** option. The currently configured default gateway shows. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad does not accept numbers 256 to 999.

6. Repeat *Step 5* to enter the correct numbers for each byte.
7. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **Address Parameters** option to enter it.
4. Press [ENTER] at the **Default Gateway** option. The current configured default gateway shows.

5. To change the setting, press the **Edit** softkey.
6. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire address. Use the softkeys and the number buttons on the keypad to enter the new address.

**NOTICE!**
The keypad does not accept invalid byte numbers.

7. Press the **Save** softkey to save the changes.

**IPv4 DNS Server IP Address**

| | |
|---|---|
| **Default:** | 0.0.0.0 |
| **Selection:** | 0.0.0.0 to 255.255.255.255 |

This This defines the address of the Doman Name Server (DNS). When this is defined through the DHCP service, leave the default value.

**Keypad Programming of IPv4 DNS Server IP Address**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **DNS PARAM** option to enter it.
4. Press [ENT] at the **SERVER ADDRESS** option. The currently configured server address shows. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. Press [PREV] to delete the characters of the byte, and then enter the new byte numbers, or press [NEXT] to move to the next byte.

**NOTICE!**
The keypad does not accept numbers 256 to 999.

6. Repeat *Step 5* to enter the correct numbers for each byte.
7. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **DNS Parameters** option to enter it.
4. Press [ENTER] at the **Server Address** option. The current configured default gateway shows.
5. To change the setting, press the **Edit** softkey.
6. The **Previous** and **Next** softkeys move the cursor through the bytes. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire address. Use the softkeys and the number buttons on the keypad to enter the new address.

**NOTICE!**
The keypad does not accept numbers 256 to 999.

7. Press the **Save** softkey to save the changes.

**Port 77EE Configuration Enable**

| **Default**: | No |
|---|---|
| **Selection:** | Yes or No |
| Yes | The network module allows configuration to be sent from the network through port 77FE. |
| No | The network modules does not allow configuration to be sent from the network through port 77FE. |

Port number 77EE (hexadecimal code) is reserved for configuration of the B420 by the remote application software.

**UPnP Enable**

| **Default**: | Yes |
|---|---|
| **Selection:** | Yes or No |
| Yes | UPnP is enabled |
| No | UPnP is disabled |

Universal Plug and Play (UPnP) allows devices to connect seamlessly and simplifies the implementation of personal and corporate networks.

**Keypad Programming of UPnP Enable**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **MODULE PARAM** option to enter it.
4. Press [ENT] at the **UPnP ENABLE** option. The keypad shows YES or NO.
5. To change the setting, press [EDIT] and then press the button for the desired option.
6. Press [ENTER] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENT] to enter the **Programming** option.
3. Press [ENT] at the **Module Parameters** option to enter it.
4. Press [ENT] at the **UPnP Enable** option. The keypad shows Yes or No.
5. To change the setting, press **Edit** softkey and then press the softkey for the desired option.
6. Press the **Save** softkey to save the changes.

**HTTP Port Number**

| **Default**: | 80 |
|---|---|
| **Selection:** | 1 to 65535 |

Use this option to configure the port number for the B420 web server.

**ARP Cache Timeout**

| **Default:** | 600 |
|---|---|
| **Selection:** | 1 to 600 (in 1-sec increments) |

When the B420 communicates with any device on a network, an entry is added to its ARP table for each of those devices. The ARP Cache Timeout defines the number of seconds (1 to 600) before the ARP table of the B420 is refreshed.

### AES Encryption Enable

| **Default:** | No |
|---|---|
| **Selection:** | Yes or No |
| Yes | All communication through the network module is encrypted. AES encryption must also be set at the central station receiver and the PC running RPS or automation software. |
| No | All communication through the network module is unencrypted. |

Use this option to enable or disable AES (Advanced Encryption Standard) encryption on the B420.

### Keypad Programming of AES Encryption Enable

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **ENCRYPTION** option to enter it.
4. Press [ENT] at the **AES KEY SIZE** option. The keypad shows **NONE** or **128 BITS**. **NONE** in AES KEY SIZE is the same as **No** in RPS, whereas **128 BITS** in AES KEY SIZE is the same as **Yes** in RPS.
5. To change the setting, press [EDIT] and then press the button for the desired option.
6. Press [ENTER] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENT] to enter the **Programming** option.
3. Press [ENT] at the **Encruption** option to enter it.
4. Press [ENT] at the **AES Key Size** option. The keypad shows **None** or **128 Bits**. **None** in AES KEY SIZE is the same as **No** in RPS, whereas **128 Bits** in AES KEY SIZE is the same as **Yes** in RPS.
5. To change the setting, press **Edit** softkey and then press the softkey for the desired option.
6. Press the **Save** softkey to save the changes.

### AES Encryption Key

| **Default:** | 01-02-03-04-05-06-07-08-09-10-11-12-13-14-15-16 |
|---|---|
| **Selection:** | Thirty-two hexadecimal characters |

Use this option to select the ID that represents the AES Encryption Key to use to encrypt and decrypt data blocks. Create the ID numbers in Remote Programming Software (RPS) using the **Encryption Key** tab of the **System Configuration** dialog box.

### Keypad Programming of AES Encryption Key

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **ENCRYPTION** option to enter it.

4. Press [ENT] at the **AES ENCRYPTION KEY** option. If Encyption is disabled through RPS or keypad programming, the keypad shows **NO ENCRYPTION**. If Encryption is enabled, the default keypad value is **NO ASSIGNED VALUE**.
5. To change the setting, press [EDIT] and then enter the value using the number buttons.
6. Press [ENTER] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENT] to enter the **Programming** option.
3. Press [ENT] at the **Encryption** option to enter it.
4. Press [ENT] at the **AES Encryption Key** option. If Encyption is disabled through RPS or keypad programming, the keypad shows **No Encryption**. If Encryption is enabled, the default keypad value is **No Assigned Value**.
5. To change the setting, press **Edit** softkey and then enter the value using the number buttons.
6. Press the **Save** softkey to save the changes.

### Web Access Enable

| | |
|---|---|
| **Default:** | No |
| **Selection:** | Yes or No |
| Yes | Web configuration is enabled |
| No | Web configuration is disabled |

When enabled, the B420 allows authorized users to view and modify its configuration parameters through a standard web browser.

### Web Access Password

| | |
|---|---|
| **Default:** | B42V2 |
| **Selection:** | Four to ten alphanumeric characters |

Use this parameter to authorize web access to the B420 Network Communication Module.

**NOTICE!**
The password 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.

**NOTICE!**
To disable the password check, enter a space (using the [Spacebar] key), as the password.

### Firmware Upgrade Enable

| | |
|---|---|
| **Default**: | No |
| **Selection:** | Yes or No |
| Yes | Allows firmware upgrades to the B420 using the network. |
| No | Prevents firmware upgrades. |

Use this parameter to enable or disable firmware upgrades on the B420.

### Module Hostname (B420)

Use this parameter to create a module hostname. This is the hostname that represents the module on the network. Once set, this hostname can be used to contact the control panel via RPS over network. If enabled, a web browser can connect to this communication module at this host name for the purposes of configuration and diagnostics.

**NOTICE!**
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.

| **Default**: | Blank |
|---|---|
| **Selection:** | Sixty-four alphanumeric characters |

**Keypad Programming of Unit Hostname**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.
3. Press [ENT] at the **DNS PARAM** option to enter it.
4. Press [ENT] at the **MODULE HOSTNAME** option. The currently configured hostname shows. An invisible editing cursor is enabled for the first byte.
5. The [PREV] button acts as a [Backspace] key. The [COMMAND] key allows you to cycle though the special passcode characters (A, B, C, D, E, F); the [NEXT] key selects the passcode character.
6. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **DNS Parameters** option to enter it.
4. Press [ENTER] at the **Module Hostname** option. The current configured hostname shows.
5. To change the setting, press the **Edit** softkey. An invisible editing cursor is enabled.
6. Use the softkeys and the number buttons on the keypad to enter the new passcode. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entire passcode. When entering a letter character, press the letter's softkey to select it. The **Previous** and **Next** softkeys advance through the letter characters (A, B, C, D, E, F).
7. Press the **Save** softkey to save the changes.

**Unit Description**

Use this parameter to create a unit description.

**NOTICE!**
The description 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.

| **Default**: | Blank |
|---|---|
| **Selection:** | Twenty alphanumeric characters |

**Local Port Number**

| **Default:** | 7700 |
|---|---|
| **Selection:** | 0 to 65535 |

**Keypad Programming of Local Port Number**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **PROGRAMMING** option.
2. Press [ENT] to enter the **PROGRAMMING** option.

3. Press [ENT] at the **ADDRESS PARAM** option to enter it.
4. Press [ENT] at the **PORT NUMBER** option. The currently configured port number shows.
5. Press [ENT] to change the port number. An editing cursor is enabled.
6. The [PREV] button acts as a [Backspace] key. Enter the desired port number using the number buttons.
7. Press [ENT] to save the changes.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Programming** option.
2. Press [ENTER] to enter the **Programming** option.
3. Press [ENTER] at the **Address Parameters** option to enter it.
4. Press [ENTER] at the **Port Number** option. The current configured port number shows.
5. Press the **Edit** softkey to change the port number. An editing cursor is enabled.
6. The **Previous** and **Next** softkeys move the cursor through the number. The **Backspace** softkey allows you to erase characters. The **Clear** softkey allows you to clear the entered numbers. Use the softkeys and the number buttons on the keypad to enter the new port number.
7. Press the **Save** softkey to save the changes.

### TCP Keepalive Time

| | |
|---|---|
| **Default:** | 45 |
| **Selection:** | 0 to 65 (in 1-sec increments) |

### IP Test Address

**NOTICE!**
Domain Name characters are in accordance with RFC 1123 Requirements for Internet Hosts -- Application and Support.

| | |
|---|---|
| **Default:** | 8.8.8.8 |
| **Selection:** | Twenty alphanumeric characters |

This is the test address that the network module will use when the **IP Diagnostics** tests are activated from the keypad’s **Tools Menu.** The network address in this prompt is decoded and an ICMP ping message is sent during the test so set this to an address that allows this form of communication. You can enter an intranet address if you do not wish the system to test an external IP address. Refer to *Section 8.3.1 IP Diagnostics Keypad Menu (B420), page 189* for further details.

**NOTICE!**
For systems reporting over the internet, the test address can be set to a web server with fast response time and high availability. This verifies that the Ethernet Communicator has at least a limited internet connection outside the facility.
For all systems, including those that report only on private internal networks, the internet test address can be pointed to a server or receiver in the central station. This will verify that the Ethernet Communicator has at least a limited Ethernet connection to the specific site or receiver to which reports will be sent. For example, receiver-01.your-company-domain.com.

## 8.3.1 IP Diagnostics Keypad Menu (B420)

**Settings**

**D1255**

1. Refer to *Section 2.5.6 IP Diagnostics Menu, page 16* to access the **TOOLS MENU** and navigate to the **IP DIAGNOSTICS** option.
2. Press [ENT] to enter the **IP DIAGNOSTICS** option.
3. At the **B420 MOD 1-2** option, enter the number for the B420 module for which you want to review the settings, and press [ENT].
4. Press [ENT] at the **SETTINGS** option. The keypad shows the Hostname.
5. Press [NEXT]. The keypad shows the MAC ID.
6. Press [NEXT]. The keypad shows the current IP address assigned to the module.
7. Press [ESC] when finished reviewing the settings.

**D1260**

1. Refer to *Section 2.5.6 IP Diagnostics Menu, page 16* to access the **Tools Menu** and navigate to the **IP Diagnostics** option.
2. Press the corresponding soft button to enter the **IP Diagnostics** option.
3. At the **B420 Module 1-2** option, enter the number for the B420 module for which you want to review the settings, and press [ENTER].
4. Press [ENTER] at the **Settings** option. The keypad shows the Hostname.
5. Press the **Next** soft button. The keypad shows the MAC ID.
6. Press the **Next** soft button. The keypad shows the address assigned to the module.
7. Press the **Exit** soft button when finished reviewing the settings.

**Connection Test**

**NOTICE!**
You must configure an **IP Test Address** in RPS to test the Internet function. If the **IP Test Address** is not configured, the Internet test results in failure. Refer to *Section  IP Test Address, page 188*.

**D1255**

1. Refer to *Section 2.5.6 IP Diagnostics Menu, page 16* to access the **TOOLS MENU** and navigate to the **IP DIAGNOSTICS** option.
2. Press [ENT] to enter the **IP DIAGNOSTICS** option.
3. At the **B420 MOD 1-2** option, enter the number for the B420 module for which you want to review the settings, and press [ENT].
4. Press [ENT] at the **CONNECTION TEST** option. The keypad tests and shows the results for:
   - Link. Tests the network cable connection, and responds with **OK** or **FAILURE**.
   - Gateway. Tests the connection to the gateway, and responds with **OK** or **FAILURE**.
   - Internet. Tests the network cable connection, and responds with **OK** or **FAILURE**.

**D1260**

1. Refer to *Section 2.5.6 IP Diagnostics Menu, page 16* to access the **TOOLS MENU** and navigate to the **IP DIAGNOSTICS** option.
2. Press the corresponding soft button to enter the **IP Diagnostics** option.
3. At the **B420 Module 1-2** option, enter the number for the B420 module for which you want to review the settings, and press [ENTER].

4. Press [ENTER] at the **Connection Test** option. The keypad tests and shows the results for:
   - Link. Tests the network cable connection, and responds with **OK** or **Failure**.
   - Gateway. Tests the connection to the gateway, and responds with **OK** or **Failure**.
   - Internet. Tests the network cable connection, and responds with **OK** or **Failure**.

## 8.4 B820 SDI2 Inovonics Interface Module

The B820 SDI2 Inovonics Interface Module provides the control panel with a wireless interface for RF points, Key Fobs and RF Wireless Repeaters. This device is only supported on the SDI2 bus.

| D9412GV4 | D7412GV4 | D7212GV4 |
|---|---|---|
| 1 | 1 | 1 |

**Table 8.4** B820 Module Capacities Per Control Panel

RPS supports the configuration of the enclosure tamper on each of the B820 Inovonics Interface modules. Refer to *Section Enclosure Tamper, page 179*.

**System Supervision Time**

| | |
|---|---|
| **Default**: | 4 hours |
| **Selection:** | 0, 4 hours, 12 hours, 24 hours, 48 hours, 72 hours |
| None | No wireless device supervision |
| 4 hr | Send a missing condition after 4 hr of no contact from the wireless repeaters. |
| 12 hr | Send a missing condition after 12 hr of no contact from the wireless repeaters. |
| 24 hr | Send a missing condition after 24 hr of no contact from the wireless repeaters. |
| 48 hr | Send a missing condition after 48 hr of no contact from the wireless receiver. |
| 72 hr | Send a missing condition after 72 hr of no contact from the wireless receiver. |

Select the RF device supervision interval. If no communication has been received from a device within the configured amount of time, a device missing trouble will be generated.

**NOTICE!**

For fire devices, the control panel sets System Supervision Time to 4 hours by default, and RPS cannot change that setting. Modifying the selection in RPS for fire devices has no impact on the programming.

**Low Battery Resound**

| | |
|---|---|
| **Default:** | Never Resound |
| **Selection:** | Never Resound, 4 hours, 24 hours |

Select the amount of time to wait before resounding a persisted Low Battery trouble.

**NOTICE!**

For fire devices, the control panel sets Low Battery Resound to 24 hours by default, and RPS cannot change that setting. Modifying the selection in RPS for fire devices has no impact on the programming.

## 8.5 Wireless Repeater

The Wireless Repeater is a device that is independent of the SDI2 bus. It provides an ability to extend the range of the B820 SDI2 Inovonics Interface Module.

| D9412GV4 | D7412GV4 | D7212GV4 |
|---|---|---|
| 8 | 8 | 8 |

**Table 8.5** Wireless Repeater Capacities Per Control Panel

RPS supports the configuration of the enclosure tamper on each of the wireless repeater modules. Refer to *Section Enclosure Tamper, page 179*.
RPS supports the configuration of the RFID for each of the wireless repeater modules.

**NOTICE!**
Even though the Wireless Receiver configuration is listed under the SDI2 Modules category they are not physically connected to the SDI2 bus. They require that a B820 SDI2 Inovonics Interface Module be configured as part of the system.

**RFID Wireless Repeaters**

| | |
|---|---|
| **Default:** | 0 |
| **Selection:** | 0 - 99999999 |

RFID (Radio Frequency device IDentification number). This is a unique number assigned to a wireless device at the factory. It provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting. Since the Wireless Repeater is a receiver as well as a transmitter it also is assigned an RFID so that the Wireless Receiver can determine what Repeater is transmitting.
This RFID number is typically read off of the label that is affixed to the device. The label location may differ for each RF device.

## 8.5.1 RF Repeaters Keypad Menu (RFID Wireless Repeaters)

**Add Repeater**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF REPEATERS** option.
2. Press [ENT] to enter the **RF REPEATERS** option.
3. Press [ENT] to enter the **ADD REPEATERS** option.

**NOTICE!**
Attempting to enter a repeater with an assigned RFID generates an error tone.

4. At the **REPEATER 1-8** option, enter repeater number you wish to configure and press [ENT] or scroll through the list of available repeater numbers by pressing [NEXT]. **RFID: NOT ASSIGNED** shows.
5. Press [ENT]. The keypad indicates a transmission to the device.
6. Press the RESET button on the repeater to add it. The keypad reads **REPEATER ADDED.**

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Repeaters** option.
2. Press [ENT] to enter the **RF Repeaters** option.
3. Press [ENT] to enter the **Add Repeaters** option.

**NOTICE!**
Attempting to enter a repeater with an assigned RFID generates an error tone.

4. At the **Repeater 1-8** option, enter repeater number you wish to configure and press [ENTER] or scroll through the list of available repeater numbers by pressing the **Next** softkey. **RFID: Not Assigned** shows.
5. Press [ENTER]. The keypad indicates a transmission to the device.
6. Press the RESET button on the repeater to add it. The keypad reads **Repeater Added.**

**Replace Repeater**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF REPEATERS** option.
2. Press [ENT] to enter the **RF REPEATERS** option.
3. At the **REPEATER 1-8** option, enter the repeater number you wish to configure and press [ENT] or scroll through the available devices to replace, press [NEXT], and then press [ENT] when the RF repeater you wish to replace shows.

**NOTICE!**
You must directly enter in a RF Repeater number (2) that has an assigned RFID. Attempting to enter a repeater, without an assigned RFID will generate error tone.

4. If repeaters are available for adding as a replacement, a list of repeaters shows. To scroll through the available repeaters to add, press [NEXT], and then press [ENT] when the desired repeater shows.
5. The keypad indicates a transmission to the device. Press the RESET button on the device to add it. The keypad reads **REPEATER ADDED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Repeaters** option.
2. Press [ENT] to enter the **RF Repeaters** option.
3. At the **Repeater 1-8** option, enter the repeater number you wish to configure and press [ENTER] or scroll through the available devices to replace, press the **Next** softkey, and then press [ENTER] when the RF repeater you wish to replace shows.

**NOTICE!**
You must directly enter in a RF Repeater number (2) that has an assigned RFID. Attempting to enter a repeater, without an assigned RFID will generate error tone..

4. If repeaters are available for adding as a replacement, a list of repeaters shows. To scroll through the available repeaters to add, the **Next** softkey, and then press [ENTER] when the desired repeater shows.
5. The keypad indicates a transmission to the device. Press the RESET button on the device to add it. The keypad reads **Repeater Added**.

**Remove Repeater**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF REPEATERS** option.
2. Press [ENT] to enter the **REMOVE REPEATERS** option.
3. At the **REPEATER 1-8** option, enter the repeater number you wish to remove and press [ENT] or scroll through the available devices to remove by pressing [NEXT], and then

press [ENT] when the RF repeater you wish to remove shows. he keypad reads **RF REPEATER REMOVED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Repeaters** option.
2. Press [ENT] to enter the **Remove Repeaters** option.
3. At the **Repeater 1-8** option, enter the repeater number you wish to remove and press [ENT] or scroll through the available devices to remove by pressing the **Next** softkey, and then press [ENT] when the RF repeater you wish to remove shows. he keypad reads **RF Repeater Removed**.

### 8.5.2 RF Diagnostics Keypad Menu (RFID Wireless Repeaters)

**RF Points -- States**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF DIAGNOSTICS** option.
2. Press [ENT] to enter the **RF DIAGNOSTICS** option.
3. Press [ENT] at the **RF POINTS** option to enter it.
4. Press [ENT] to enter the **STATES** option.
5. Press [NEXT]. Within the **STATES** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - STATE
   - TAMPER
   - LOW-BATTERY
   - MAINTENANCE

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Diagnostics** option.
2. Press [ENTER] to enter the **RF Diagnostics** option.
3. Press [ENTER] at the **RF Points** option to enter it.
4. Press [ENTER] to enter the **States** option.
5. Press the **Next** softkey. Within the **States** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - State
   - Tamper
   - Low-Battery
   - Maintenance

**RF Points -- Signal Strengths**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF DIAGNOSTICS** option.
2. Press [ENT] to enter the **RF DIAGNOSTICS** option.
3. Press [ENT] to enter the **SIGNAL STRENGTHS** option.

4. Press [NEXT]. Within the **SIGNAL STRENGTHS** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - STRENGTH
   - LEVEL
   - MARGIN

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Diagnostics** option.
2. Press [ENT] to enter the **RF Diagnostics** option.
3. Press [ENT] to enter the **Signal Strengths** option.
4. Press the **Next** softkey. Within the **Signal Strengths** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - Signal Strengths
   - Level
   - Margin

**RF Repeaters - States**

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF DIAGNOSTICS** option.
2. Press [ENT] to enter the **RF DIAGNOSTICS** option.
3. Press [ENT] at the **RF REPEATERS** option to enter it.
4. Press [ENT] to enter the **STATES** option.
5. Press [NEXT]. Within the **STATES** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - TROUBLE
   - MISSING
   - TAMPER
   - LOW-BATTERY
   - AC FAIL

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Diagnostics** option.
2. Press [ENTER] to enter the **RF Diagnostics** option.
3. Press [ENTER] at the **RF Repeaters** option to enter it.
4. Press [ENTER] to enter the **States** option.
5. Press the **Next** softkey. Within the **States** option, the menu will scroll through the following sub-categories, with the results of the diagnostic check:
   - State
   - Missing
   - Tamper
   - Low-Battery
   - AC FAIL

# 9 ACCESS CONTROL (D9412GV4/D7412GV4)

This section applies only to the D9412GV4 and D7412GV4 Control Panels.

## 9.1 Door Profile

This programming category is used to:

- Assign an area that also activates the D9210C
- 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 Number**

**NOTICE!**
The D9412GV4 supports up to eight doors. The D7412GV4 supports two doors.

**D# Entry Area #**

| | |
|---|---|
| **Default:** | Disabled |
| **Selection:** | Disabled, 1 to 32 |
| 1 to 32 | The area assigned to the door controller to which the reader allows access. |
| Disabled | Door controller does not function. |

Assign an area to the door controller. This entry allows the D9210C to be polled, activating communication to the control panel. This is also the area a user exits when initiating a REX.

**NOTICE!**
The **D# Entry Area #** prompt for the D7412GV4 is limited to the first 8 areas.

**NOTICE!**
All SDI devices, regardless of area assigned, report to Area 1, Account 1 by default upon SDI failure. If a D9210C becomes disconnected, an SDI Fail ## and a Missing Point ### Event is created.

**NOTICE!**
If the D9210C is not programmed with a **D# Entry Area, 9210 NOT READY** appears at the keypad when attempting to add access credentials to a User ID.

**D# CC# Scope**

| | |
|---|---|
| **Default:** | 1 |
| **Selection:** | Disabled, 1 to 16 (for D9412GV4), 1 to 8 (for D7412GV4) |
| 1 to 16 | Determines the scope of areas to affect the access disarm request if enabled. Also, determines the keypad to be used when performing Dual Authentication. |
| Disabled | Only the area assigned in D# Entry Area is disarmed if the user has access disarm rights. No keypad assignment prohibits Dual Authentication. |

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 (128-131 on the D7412GV4) |
| 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 3.12 User Interface, page 93*) 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.

**NOTICE!**
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 *Section 3.12 User Interface, page 93*.

*Table 9.1, Page 196* shows how this programming affects custom function activation.

| **L## Function Level?** | **Custom Function Activation** |
|---|---|
| **M**<br>(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**<br>(Disarmed) | User token activates the custom function assigned to the Door Controller only while the entry area for the Door Controller is disarmed. |
| C<br>(Armed and Disarmed) | User token activates the custom function assigned to the Door Controller regardless of the armed state of the entry area. |
| - | User token does **not** run the custom function assigned to the Door Controller. |

**Table 9.1** Effects of Programming on Custom Function Activation

**NOTICE!**
A user’s security level must have an M, P, or D to operate the custom function.

### D# Door Point

| **Default:** | 0 |
|---|---|
| **Selection:** | 0 to 127, 129 to 247 (0 to 75 on the D7412GV4) |
| 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. |
| 0 | 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 so the corresponding **P### Point Source** prompt is set to **Door Point** automatically.

**NOTICE!**
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.

**NOTICE!**
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, OctoPOPIT points, Octo-input points, or RF 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:** | 0 |
| **Selection:** | 0 to 127, 129 to 247 (0 to 75 on the D7412GV4) |
| 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. |
| 0 | 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.

**CAUTION!**
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.

**NOTICE!**
The unlocked state activated by Auto Door operation 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.

**NOTICE!**
Doors that are activated by Fire Unlock must be returned to normal using the Door Control function on the keypad.

**CAUTION!**
This command unlocks the door regardless of the armed state.

**NOTICE!**
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. If **D# Door Point** is set to **0**, then this prompt is treated as if it were set to **No**. |

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).

## 9.2 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.

**D# Strike Time**

| | |
|---|---|
| **Default:** | 10 sec |
| **Selection:** | 1 sec to 240 sec |
| 0 | 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:** | 0 to 240 sec |
| 0 | 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:** | 0 to 240 sec |
| 0 | 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.

**NOTICE!**
A separate buzzer is required. Many readers have an internal buzzer that is not affected by Buzz Time.

### D# Extend Time

| | |
|---|---|
| **Default:** | 10 sec |
| **Selection:** | 0 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.

**NOTICE!**
The CLOSE DOOR # display on keypad does not activate if **D# Extend Time** is set to **0**.

**NOTICE!**
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# Deactivate 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.

**NOTICE!**
In order for this function to work, a point needs to be assigned to the door.

**NOTICE!**
To Reduce False Alarms, maintain **D# Deactivate 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.

**NOTICE!**
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).

**NOTICE!**
When **RTE Shunt Only** is **Yes**, RTE Events are not logged, reported, or printed.

**D# REX Shunt 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.

**NOTICE!**
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).

**NOTICE!**
When **REXShunt Only** is **Yes**, REX Events are not logged, reported, or printed.

## 9.3 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.

**NOTICE!**
RTE Events require **Access Granted** to be programmed as **Yes**.

### D# Access Granted?

| | |
|---|---|
| **Default:** | Yes |
| **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.

**NOTICE!**

A successful Access Event can be started by a:

- Valid user ID
- Valid door state changed at the keypad
- Scheduled or armed state change that holds a door open
- RTE or REX

### D# No Entry?

| | |
|---|---|
| **Default:** | Yes |
| **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.

**NOTICE!**

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.

**NOTICE!**

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.

**NOTICE!**

REX Events require **D# Access Granted** to be programmed as **Yes**.

# 10 SIA CP-01 Quick Reference

| Product Name | Bosch Recommended Settings for SIA CP-01 Compliance | Shipping Default | Reference Page |
|---|---|---|---|
| Phone # | (Prefix backup phone number with Call Waiting disable command) | {Blank} | *17* |
| Duress Type | Option 3 | 0 (disabled) | *59* |
| Cancel Report | Yes | Yes | *60* |
| A# Exit Dly Time | 45 sec to 255 sec | 60 sec | *63* |
| A# Duress Enable | Yes | No | *64* |
| A# Exit Restart | Yes or No | Yes | *77* |
| A# Arm No Exit | Yes or No | Yes | *78* |
| A# Two Man Rule | No | No | *74* |
| A# Early Ambush | No | No | *76* |
| A# Exit Warning | Yes | Yes | *78* |
| A# Burg Time | 6 min to 90 min | 6 min | *67* |
| A# Alarm Bell | 1 to 128 (64), A, B, C | A (on-board alarm output) | *118* |
| A# Verify Time | 10 sec to 60 sec | 60 sec | *63* |
| CC# Entry Tone | Yes or No | Yes | *86* |
| CC# Exit Tone | Yes or No | Yes | *86* |
| CC# Abort Display | Yes or No | Yes | *87* |
| CC# Cancel Display | Yes or No | Yes | *88* |
| CC# Pass Code Enter Function | Arm/Disarm | Arm/Disarm | *83* |
| CC# Dual Authentication | No | No | *84* |
| Master Arm Instant | - | - | *94* |
| Perimeter Instant | - | - | *94* |
| L## Send Duress | - or E | E[2] | *113* |
| L## Disarm | - or E | E[2] | *103* |
| L## Passcode Disarm | - or E | E[2] | *113* |
| P## Entry Delay | 30 sec to 240 sec | 30 sec | *134* |
| P## Alarm Abort | Yes or No | Yes[3] | *145* |
| Abort Window | 15 sec to 45 sec | 30 sec | *176* |
| Passcode Length | 3 to 6 digits | Disabled | *177* |
| Swinger Count | 1 to 2 trips | 1 trip | *177* |
| Remote Warning | Yes | Yes | *177* |
| Cross Point Time | 5 to 255 sec | 20 sec | *143* |
| P## Cross Point | Yes or No | No | *143* |

[1] The SIA allowed range is 1 min to 90 min. Must additionally comply with UL requirements, refer to *Section A# Burg Time, page 67*.

[2] L14 is the default duress user index.

[3] The default for P## Alarm Abort is No for P3, P4, P5, and P22.

**Table 10.1** Programming the Control Panels for SIA CP-01 Compliance

# 11 Keypad Tools Menu (Options Not Available in RPS)

## 11.1 Service Bypass Menu

### 11.1.1 Setting Service Bypass (PT NUM 1-247)

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **SERVICE BYPASS** option.
2. Press [ENT] to enter the **SERVICE BYPASS** option.
   If no points are bypassed, **NO PTS BYPASSED** shows. Skip to *Step 6*. If points are bypassed, a list of unbypassed points shows.
3. Press [NEXT] to advance through the points in service bypass.
4. Press [ENT] to select the point that needs to have service bypass removed.
5. Press [NEXT] to toggle the **SERVICE BYPASS** setting, then [ENT] to save.
6. Press [ENT] at the **SERVICE BYPASS** prompt. The **PT NUM 1-247:** prompt shows.
7. Press the point number followed by [ENT]. The **PT-### SERVICE BYPASS: NO** prompt is shown.
8. Press [NEXT] to toggle the **SERVICE BYPASS** setting, then [ENT] to save. The keypad reads **POINT BYPASSED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Service Bypass** option.
2. Press [ENTER] to enter the **Service Bypass** option.
   If no points are bypassed, **No Points Bypassed** shows. If points are bypassed, a list of unbypassed points shows.
3. The number of points in service bypass are below the **Point Num 1-247:** prompt. Enter the point number followed by [ENTER].
4. Press [ENTER] to make a selection. The keypad reads **Point Bypassed**.

### 11.1.2 Resetting Service Bypass

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **SERVICE BYPASS** option.
2. Press [ENT] to enter the **SERVICE BYPASS** option.
   The **SERVICE BYPASS** prompt alternates with the number of points in service bypass.
3. Press [NEXT] to advance through the points in service bypass.
4. Press [ENT] to select the point that needs to have service bypass removed.
5. Press [NEXT] to toggle the SERVICE BYPASS setting, then [ENT] to save.
6. Press [ESC] at any time to return to the list of points in service bypass to select another or press [ESC] again to exit.
   When the keypad reads **PARAMETER SAVED**, your selection has been configured.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **Service Bypass** option.
2. Press [ENTER] to enter the **Service Bypass** option.
   The **Service Bypass** prompt alternates with the number of points in service bypass.

3. The number of points in service bypass display below the **Point Num 1-247:** prompt. Enter the point number followed by [ENTER] or press the **Next** softkey to advance to the point.
4. At the **Point (###) Service Bypass: Yes** prompt press the **Edit** softkey.
5. Press the **No** softkey, then press the **Save** softkey to remove service bypass.
6. Press the **Next** softkey to advance to another point, or press the **Exit** softkey to select another, or press the **Esc** softkey to exit
   When the keypad reads **Parameter Saved**, your selection has been configured.

## 11.2 RF Points Menu

### 11.2.1 Enroll RF Point

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF POINTS** option.
2. Press [ENT] to enter the **RF POINTS** option.
3. At the **ENROLL RF POINT** prompt, press the [ENT] option. If all wireless devices are enrolled, **ALL POINTS ADDED** shows. If wireless devices are available for enrolling, a list of wireless devices shows.
4. To scroll through the available devices to enroll, press [NEXT], and then press [ENT] when the desired device shows.
5. The keypad indicates a transmission to the device. Press the [RESET] button on the device to enroll it. The keypad reads **POINT ENROLLED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF POINTS** option.
2. Press [ENTER] to enter the **RF POINTS** option.
3. At the **Enroll RF Point** prompt, press the [ENTER] option. If all wireless devices are enrolled, **All Points Added** shows. If wireless devices are available for enrolling, a list of wireless devices shows.
4. To scroll through the available devices to enroll, press the **Next** softkey, and then press [ENTER] when the desired device shows.
5. The keypad indicates a transmission to the device. Press the [RESET] button on the device to enroll it. The keypad reads **Point Enrolled**.

### 11.2.2 Replace RF Point

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF POINTS** option.
2. Press [ENT] to enter the **RF POINTS** option.
3. At the **REPLACE RF POINT** prompt, press [ENT]. A list of enrolled wireless devices shows.
4. To scroll through the available devices to replace, press [NEXT], and then press [ENTER] when the RF point you wish to replace shows.
5. If wireless devices are available for enrolling as a replacement, a list of wireless devices shows. To scroll through the available devices to enroll, press [NEXT], and then press [ENT] when the desired device shows.
6. The keypad indicates a transmission to the device. Press the [RESET] button on the device to enroll it. The keypad reads **POINT ENROLLED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Points** option.
2. Press [ENTER] to enter the **RF Points** option.
3. At the **REPLACE RF POINT** prompt, press [ENTER]. A list of enrolled wireless devices shows.
4. To scroll through the available devices to replace, press the **Next** softkey, and then press [ENTER] when the RF point you wish to replace shows.
5. If wireless devices are available for enrolling as a replacement, a list of wireless devices shows. To scroll through the available devices to enroll, press the **Next** softkey, and then press [ENTER] when the desired device shows.
6. The keypad indicates a transmission to the device. Press the [RESET] button on the device to enroll it. The keypad reads **Point Enrolled**.

### 11.2.3 Remove RF Point

**D1255**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **TOOLS MENU** and navigate to the **RF POINTS** option.
2. Press [ENT] to enter the **RF POINTS** option.
3. At the **REMOVE RF POINTS** prompt, press [ENT]. A list of enrolled wireless devices shows.

**NOTICE!**
By pressing the [ENT] button inside the **REMOVE RF POINT** option, you will remove any previously programmed points, and an alarm will go off. A **NO POINTS** prompt will be displayed as a result.

4. At the following prompt (**PT-## RFID AUTO LEARNED** if the previous device was auto-learned, or **PT-##** and then the RFID) prompt, enter in the RF point number you wish to remove and press [ENT] or to scroll through the available devices to enroll, press [NEXT], and then press [ENT] when the desired device shows. The keypad reads **RF POINT REMOVED**.

**D1260**

1. Refer to *Section 2.5.1 Keypad Programming Menu, page 12* to access the **Tools Menu** and navigate to the **RF Points** option.
2. Press [ENT] to enter the **RF Points** option.
3. At the **Remove RF Points** prompt, press [ENTER]. A list of enrolled wireless devices shows.

**NOTICE!**
By pressing the [Remove] button inside the **Remove RF Point** option, you will remove any previously programmed points, and an alarm will go off. A **No Points** prompt will be displayed as a result.

4. At the following prompt (**PT-## RFID Auto Learned**) if the previous device was auto-learned, or **PT-##** and then the RFID) prompt,, enter in the RF point number you wish to remove and press [ENTER] or to scroll through the available devices to enroll, press the **Next** softkey, and then press [ENTER] when the desired device shows. The keypad reads **RF Point Removed**.

**NOTICE!**
After selecting the RF Point for removal the panel instructs the Commercial Wireless module to delete the device. The point’s RFID is unassigned and saved.

**Bosch Security Systems, Inc.**
130 Perinton Parkway
14450 Fairport, NY
USA
**www.boschsecurity.com**