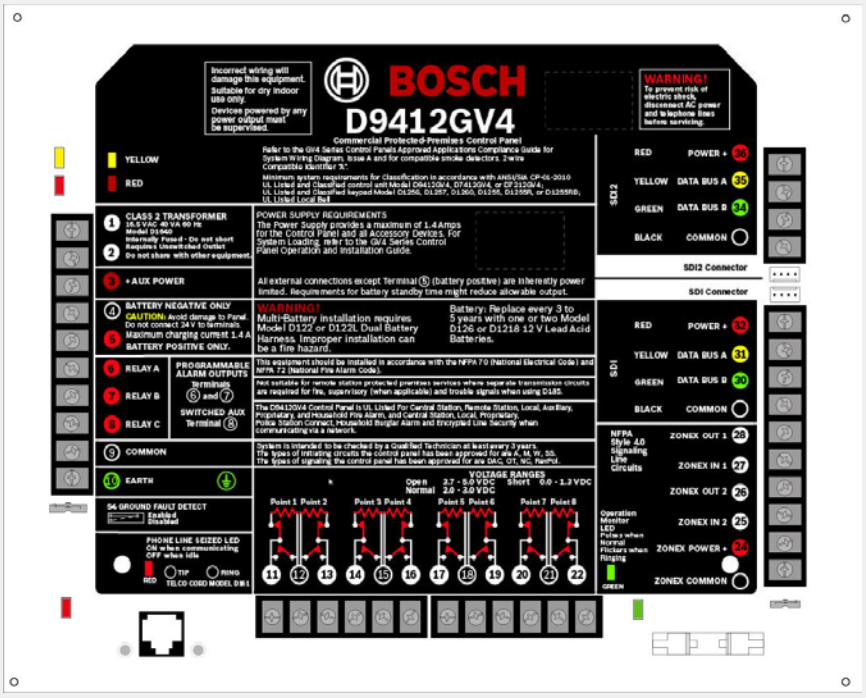


Control Panels

D9412GV4/D7412GV4 v2.03

en Program Entry Guide

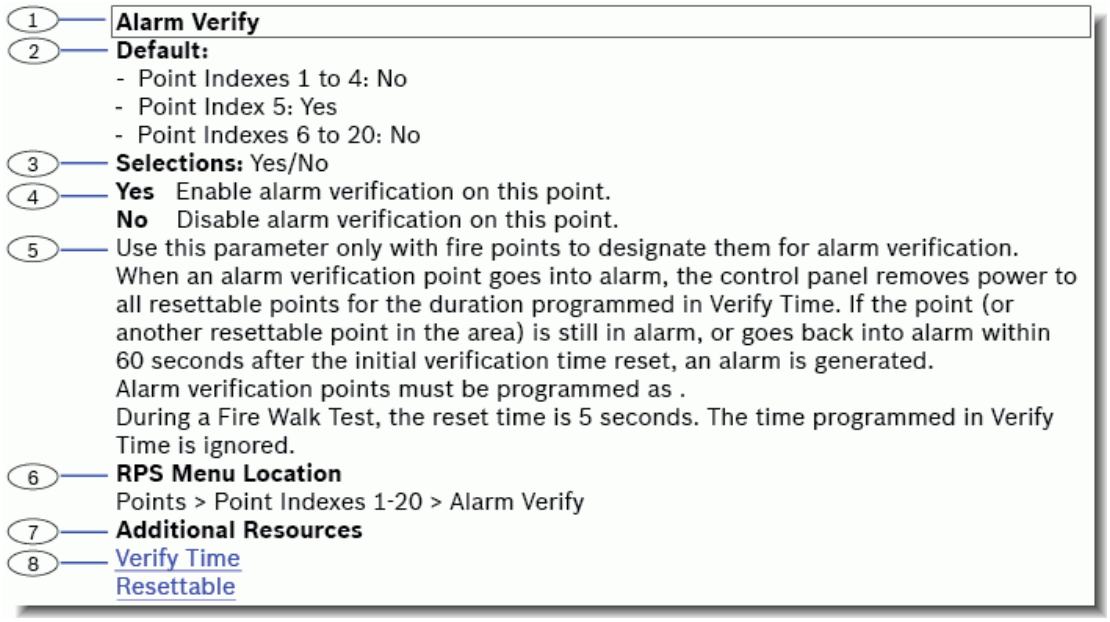
Table of Contents

1 Introduction

1.1 The Program Entry Guide

Guide to programming options

You must use RPS to fully program the control panel. You can use the limited keypad Installer menu 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. A description of each parameter and its programming options is presented in the following manner:



Callout	Description
1	The parameter. Each parameter shows exactly as it appears in the Remote Programming Software (RPS).
2	Parameter default setting. Because defaults are set for the typical installation, programming each parameter might not be necessary. Review the default entries in this document to determine which parameters you must program.
3	Parameter selections. For a particular program item, you can use only the listed selections.
4	Selection descriptions. Read the selection descriptions carefully to determine the desired action for this parameter and avoid improperly

Callout	Description
	programmed equipment.
5	Parameter description. The parameter description provides a general understanding of the function this parameter performs.
6	RPS menu location. Locate this parameter in RPS by following the menu path listed here.
7	Additional resources. Topics related to this parameter are listed here.
8	Links. Jump to the listed topics by clicking on the links provided or access information on the topics quickly by referencing the topics in the Table of Contents.

Guide to UL 864 Programming Requirements

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

IMPORTANT

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.

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864
If using two phone lines:			
Phone 1 through 4	Yes	24 characters	Program a valid phone number
Phone Supervision	Yes	0 to 240 sec	10 to 200 sec
Alarm On Fail	No	Yes / No	Set to No
Two Phone Lines	Yes	Yes / No	Set to Yes when using PSTN communications
Expand Test Report	Yes	Yes/No	Set to Yes
Fire Reports	Yes	Yes / No	Set to Yes
Fire Supervisory Missing	Required	Yes/No	Set to Yes
Test Reports	Yes	Yes / No	Set to Yes

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864
AC Fail Report	Yes	Yes / No	Set to Yes
AC Restoral Report	Yes	Yes / No	Set to Yes
Battery Missing Report	Yes	Yes / No	Set to Yes
Low Battery Report	Yes	Yes / No	Set to Yes
Battery Restoral Report	Yes	Yes / No	Set to Yes
AC Fail Time	Yes	1:00 to 90:00 min	Enter 1:00
AC Fail Display	Yes	10 to 300 sec	10 to 200 sec
AC Tag Along	Yes	Yes / No	Set to Yes
AC/Battery Buzz	Yes	Yes / No	Set to Yes
Bat Fail/Restoral Report	Yes	Yes / No	Set to Yes
Service Start Report	Required	Yes / No	Set to Yes
Service End Report	Required	Yes / No	Set to Yes
Fire Walk St Report	Required	Yes / No	Set to Yes
Fire Walk End Report	Required	Yes / No	Set to Yes
Walk Test St Report	Required	Yes / No	Set to Yes
Walk Test End Report	Required	Yes / No	Set to Yes
AC Fail Time	Yes	1:00 to 90:00 min	Enter 1:00
AC Fail Display	Yes	10 to 300 sec	10 to 200 sec
AC Tag Along	Yes	Yes / No	Set to Yes
AC/Battery Buzz	Yes	Yes / No	Set to Yes
Bat Fail/Restoral Report	Yes	Yes / No	Set to Yes
Area 1 Area On	Required to send system status reports	Yes / No	Set to Yes
Delay Restoral	Yes	Yes / No	Set to Yes
Restart Time	Yes	10 to 60 sec	60 sec
Area # Fire Time	Yes	1 to 90 min	5 min (check with AHJ)
Supervised	Yes	Yes / No	Set to Yes
Trouble Tone	Yes	Yes / No	Set to Yes
Scroll Lock	Yes	Yes / No	Set to Yes
Remote Program	Disable /Enable	-, E, or P	Set to P

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864
Fire Bell	Yes	0 to 128, A, B, C0 to 128, A, B, C	Program with a relay
Reset Sensors	Yes		Program with a relay
Area # Auth	Yes	0 to 8	Program an Authority Level for the Fire Area
Passcode	Yes	3-, 4-, 5-, or 6-digit passcode	Must program at least one passcode
Silent Bell	No	Yes / No	Set to No
Invisible Point	No	Yes / No	Set to No
Local While Disarmed	No	Yes / No	Set to No
Local While Armed	No	Yes / No	Set to No
Disable Restorals	No	Yes / No	Set to No
Bypassable	No	Yes / No	Set to No
Swinger Bypass	No	Yes / No	Set to No
Fire Point	Yes	Yes / No	Set to Yes
Resettable	Yes	Yes / No	As required
Function Code	Required	1 to 11, 13 to 28	Sked Function Code 9
Defer Test	No	Yes / No	Set to No
Hourly Test(Report?)	No	Yes / No	Set to No
Time	Enter valid time	00:00 to 23:59	00:00 to 23:59
Date	No	mm/dd	Set to No
Sunday	Yes	Yes / No	Set to Yes
Monday	Yes	Yes / No	Set to Yes
Tuesday	Yes	Yes / No	Set to Yes
Wednesday	Yes	Yes / No	Set to Yes
Thursday	Yes	Yes / No	Set to Yes
Friday	Yes	Yes / No	Set to Yes
Saturday	Yes	Yes / No	Set to Yes
Xept On Holiday	No	Yes / No	Set to No
For IP Communications to a D6600 Receiver			
Enhanced Comm	Yes	Yes / No	Set to Yes
Path1 IP Add1 (2, 3 or	Yes	000 to 255	Program a valid IP

Product Feature/Option	Permitted in UL 864? (Y/N)	Possible Settings	Settings Permitted in UL 864
4)			address
Path 1 Poll Rate	Yes	0, 5 to 65535 sec*	Program as necessary
Path 1 Ack Wait	Yes	0, 5 to 65535 sec*	Program as necessary
Path 1 Retry Count	Yes	0 to 255	Program as necessary
Receiver Supervision Time	Yes	0, 5 to 65535 sec	Program as necessary
For Ground Fault Enable Switch			
(Refer to the D9412GV4/D7412GV4 /D7212GV4 Operation and Installation Guide			
(P/N: F01U201527)	Yes	Closed = Enabled	
Open = Disabled	Closed	N/A	
* Set the Path 1 Poll Rate to 65535 for 24 hr.			

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

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
Scope	Panel Wide, Account Wide, Area Wide, Custom, No Keypad	Do not program No Keypad
Enhanced Keypad	Yes / No	Set to Yes, if applicable
Menu Key Lock	Yes / No	If using D1256RB, set to No
Reset Sensors	Disable/Enable/Passcode	Enable

Prompt	Possible Settings	Recommendations
	Protect	
Fire Test	Disable / Enable / Passcode Protect	Enable
Reset Sensors	Disable / Enable	If Reset Sensor is set to Passcode Protect, set this to Enable
Fire Test	Disable / Enable	If Fire Test is set to Passcode Protect, set this to Enable
User Group	0 to 8	Program as 0
Ring Until Restored	Yes / No	May be required for Waterflow, otherwise No
Cross Point	Yes / No	Set to No for Fire devices.
Fire Unlock	Yes / No	No

Required Programming to meet UL 636

When using a B Series control panel for hold-up operation, a hold-up point should have the following setting applied to it:

– Point Type = 0 (Point is constantly armed regardless of the status of the system.)
– Invisible Point = Yes (Keypads do not show alarm activity from this point.)

When using Modem 4 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.)

Required Programming for UL and ULC Applications

Requirement	Parameter
Acknowledge signal (ringback) shall be enabled for commercial burglary	Area Wide Parameters > Bell Test set to Yes
Remote programming requires on-site authorization (UL only)	Panel Wide Parameters > RPS Parameters > Answer Armed and Answer Disarmed set to 0 (zero) User Configuration > User Function > Remote Program set to P (passcode required) User Configuration > Authority Levels > Remote Program set to E (enabled)
Remote programming shall be disabled (ULC	Panel Wide Parameters > RPS Parameters > Answer

Requirement	Parameter
only)	Armed and Answer Disarmed set to 0 (zero) User Configuration > User Function > Remote Program set to - (disabled)
Minimum bell time is 4 min (Residential Burglary)	Area Wide Parameters > Burg Time set to 4 or greater
Minimum bell time is 15 min (Commercial Burglary, UL)	Area Wide Parameters > Burg Time set to 15 or greater
Minimum bell time is 30 min (Commercial Burglary, ULC)	Area Wide Parameters > Burg Time set to 30 or greater
Minimum bell time is 4 min (Residential Fire, UL)	Area Wide Parameters > Fire Time set to 4 or greater
Minimum bell time is 5 min (Residential Fire, ULC)	Area Wide Parameters > Fire Time set to 5 or greater
24-hr check-in (test report) enabled (Commercial Burglary, PSTN communications)	Schedules > Function set to Send Test Report Schedules > Time set to desired time of day to send Test Report Schedules > Sunday through Saturday set to Yes
Keypad manual alarms (emergency keys) shall not be enabled	Keypads > Global Keypad Settings > A Key Response, B Key Response, and C Key Response not set to Manual Alarm
AC Fail Delay is 1 min	Panel Wide Parameters > Power Supervision > AC Fail Time set to 01:00
AC Fail display delay maximum is 200 sec	Panel Wide Parameters > Power Supervision > AC Fail Display set to 200 sec or less
Alarm Abort delay (window) and entry delay combined shall not exceed 60 sec	Panel Wide Parameters > Miscellaneous > Abort Window and Points > Point Indexes > Entry Delay combined less than or equal to 60 sec
Exit Delay Maximum is	Area Wide Parameters > Exit Delay Time set to less

Requirement	Parameter
120 sec	than or equal to 120 sec
Entry Delay Maximum is 45 sec (Residential Burglary)	Points > Point Indexes > Entry Delay set to 45 sec or less
Entry Delay Maximum is 60 sec (Commercial Burglary)	Points > Point Indexes > Entry Delay set to 60 sec or less
Off Board relays shall not be used for alarm output	Output Parameters > Area Wide Outputs > Alarm Bell and Fire Bell set to A(1), B(2), C(3), or 0 only
Fire Zones shall not be cross zoned	Points > Point Indexes > Point Type set to Fire Point and Cross Point set to No
Reset sensors shall not be disabled for fire applications	User Configuration > User Function > Reset Sensors set to E (enabled) or P (passcode required) User Configuration > Authority Levels > Reset Sensors set to E (enabled)
Local while Armed shall be disabled for UL 1076, UL 1610, UL 636, and ULC S304 applications	Points > Point Indexes > Local while Armed set to No
Entry Delay shall be audible	Keypads > SDI2 Keypad Assignments > Entry Delay set to Yes

Required values to achieve 180s (ULC)/200s (UL) supervision interval

Requirement	Parameter
Supervision interval for IP communication is 200 seconds (UL)	Panel Wide Parameters > Enhanced Communications > Poll Rate set to 140, ACK Wait Time set to 10, and Retry Count set to 5
Supervision interval for IP communication is 180 seconds (ULC)	Panel Wide Parameters > Enhanced Communications > Poll Rate set to 140, ACK Wait Time set to 10, and Retry Count set to 5

1.2 About Documentation

Copyright

Trademarks

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

1.3 About product date codes

Use the serial number located on the product label and refer to the Bosch Security Systems, Inc. web site at http://www.boschsecurity.com/datecodes/.

2 Panel Specific Information

Virtual Inputs and Outputs

When is a point Virtual?

A point is virtual when its Point Source parameter is set to **Output**.
When Point Source is set to Output, the output with the same number is virtually connected to the point. There are no physical connections when a point is virtual. Whenever the output is activated, the control panel creates a fault (open circuit) for the point. Points with their Point Source set to Output can never be in a short circuit or missing state.

When is an output virtual?

An output is virtual when its Output Source parameter is set to **Zonex** and the point with the same number (Point 11 and Output 11 for example) has it's Point Source set to Output and an octo-output module is not connected.
When Output Source is set to Zonex and there is no connection to an octo-output module, the output and the point with the same number are virtually connected. They are not physically connected.
When a point is virtually connected to the output of the same number, the output does not have to be virtual as well. Its Output Source parameter can be set to either Zonex or Octo-Output.

IMPORTANT
You cannot program an output that is the Point Source for the point with the same number (Point 11 and Output 11 for example) to an output function that would cause the point to reactivate itself.

Configuring a Virtual Output

Valid Number Range

	D9412GV4	D7412GV4
Available virtual output numbers	9-128	9-64
Available virtual point numbers	9-128	9-64

Note: The number range 1-8 is unavailable for virtual inputs and virtual outputs because on-board points cannot have their source changed.

Operation and Usage

Virtual Inputs (Points)

- A virtual input is set to **open circuit state** by an activating output of the same number. The activating output can be located on any source; virtual output, on-board output, Octo-output, or Keypad-output.
- Virtual inputs can only be in an open circuit or normal circuit state. They are never in a short circuit or missing state.
- Virtual inputs can be queried by the appropriate point status commands in execute function and automation protocols.

Virtual Outputs

- A virtual output is prohibited by the control panel software from activating an input that will directly reactivate itself.

Example: A virtual point configured with Output Follows Point.

Example: A virtual watch point activated by the watch output of the same area.

- Any output prompt in the control panel can be configured with a virtual output number.
- A virtual output configured as an area-wide Fire, Gas or Burglar alarm output follows the associated bell pattern.
- All Sked and Custom Function output functions (Set Output, Reset Output, Toggle Output, and One-Shot output) can be configured with virtual output numbers.
- Since Virtual outputs and Zonex outputs are considered the same on the GV4 control panel, they must follow the same pattern restrictions. This means the temporal 4 pattern is played at a slower rate.
- Virtual outputs can be set, reset or queried by the appropriate output commands in execute function and automation protocols.

Programming Notes

IMPORTANT

After system installation and any control panel programming, perform a complete system test (a UL864 requirement). A complete system test includes testing the control panel, all devices, and communication paths for proper operation.

- When deleting Site Codes and Card Data, delete the Card Data first, then change the Site Code to 255 (blank).
- Up to five digits may be entered in the Access Card Data displayed in RPS.
- When User Code Change, Card Assigned, User Level Set and User code Delete events are uploaded into RPS, who performed the function is displayed (as long as these commands are passcode protected in Keypad Functions), but who is affected is not displayed.

GV4 Modem Compatibility List

IMPORTANT: The modem initialization strings have been tested and currently work as described below. The modem manufacturers, however, reserve the right to change specifications without notice. This can cause unexpected results when communicating with the control panel.

Modem	Init String	Reset String	Additional Settings	NOTE
Best Data 56SX	AT%Q0%C0\N0S7=255S37=3		Add ;ATA at the end of the control panel phone number to turn on Answer Mode after dialing the control panel.	The number of rings until the control panel answers must be set to between 2 and 3 rings in order to catch the correct communications handshake tone. The user can also initiate remote handshaking at the control panel keypad with MENU 34, but it must be done within a few moments after the modem dials the control panel.
Hayes	ATX0S7=255	AT&F	If using callback,	• Modems with firmware

Modem	Init String	Reset String	Additional Settings	NOTE
SMARTMODEM 1200			make sure the control panel is programmed to answer on one ring. The init string above must be changed from S10=254 to S10=255.	version lower than 136 might not operate as expected and might cause erratic communication results. To display the modem firmware version, choose “Direct Connect” in Hyper Terminal, type “ATI0”, and press the Enter key. • Various versions of this modem might cause intermittent connection problems. DIP Switches*: UP: 1, 2, 4, 6, 7 DOWN: 3, 5, 8
Hayes SMARTMODEM 2400	AT&C1&D2X0&Q0S7=255	AT&F		This init string was tested on modem firmware version 249. To display the modem firmware version, choose “Direct Connect” in Hyper Terminal, type “ATI0”, and press the Enter key. DIP Switches*: UP: 1, 2, 4, 6, 7 DOWN: 3, 5, 8
Hayes Accura 14400 + Fax 144 Model: 5300AM	ATB1N0X0&Q0S7=255S37=3	AT&F		
Practical Peripherals PM144MT II with RI LED	ATB1N0&Q6&K0S7=255S37=3S36=1S46=0	AT&F	Add ;ATA at the end of the control panel phone number to prevent the control panel from disconnecting.	

Modem	Init String	Reset String	Additional Settings	NOTE
Practical Peripherals PM144MT II with AA LED	ATB1N0&Q6&K0 S7=255S37=3S3 6=1S46=0	AT&F		
Securcomm by DC Security Model DL110	ATX0&Q0S7=255	AT&F		
US Robotics Sportster 56K	ATX0&B0&H0&K0 &M0&N2&U2S7= 255	AT&F		• The control panel cannot answer before 2 rings and must answer within 9 rings. • If using an external modem connection, change the init string sequence from “N1S7” to “N6S7” to include data transfer at 9600 Baud. Make sure the Baud rate setting in the Panel Communication screen is also set to 9600. Refer to the modem and control panel installation/programming instructions for more information. DIP Switches*: UP: 1, 2, 4, 6, 7 DOWN: 3, 5, 8
ZOOM VFX-28.8	ATN0%C0\N0&Q S7=255S37=1	AT&F	Add ;ATA at the end of the control panel phone number to turn on Answer Mode after dialing the control panel.	DIP Switches*: If available – may vary by modem version. Some modems contain 10 DIP switches. If this is the case, Switches 9 & 10 should be in the UP position.

3 Panel Wide Parameters

3.1 Phone and Phone Parameters

Phone 1, 2, 3, 4

Default: Blank
Selections: Up to 24 characters (do not enter SPACE)
Enter the telephone number that the control panel dials to contact the central station receiver when sending reports.
0 - 9: Numbers 0 through 9
C: 3-second pause
D: 7-second dial tone detect
 # 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.
The control panel is pre-programmed with a 7-second dial tone detect period. When dial tone is detected or the waiting period ends, the panel begins to dial. To extend the dial tone detect program, 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 Modem4 ACK tone from the central station receiver, program extra Cs after the phone number. The control panel waits on line for three extra seconds for each C programmed.
The first line of the phone number data entry line must be filled (12 characters) before you press ENTER to move on to the second line. If you enter characters on the second line, and there are less than 12 characters on the first line, the second line clears when you press ENTER.

IMPORTANT:

- Leaving this parameter blank does not disable phone routing. To disable reporting to this phone, see Routing.
- When dialing the central station using an ITS-DX4020-G in GSM mode, the control panel must dial the **C** character before the central station's phone number. This ensures that the control panel will dial a continuous string of numbers to reach the central station instead of pausing after the first digit to check for DTMF or pulse dialing.
- When using PSTN telephone lines, you must program two telephone numbers to meet UL864 requirements.
- To comply with SIA CP-01 False Alarm Reduction, ensure that backup telephone reporting number is programmed to disable Call Waiting (typically ***70 pause**) if Call Waiting is used. See SIA CP-01 Verification for more information.
- If you program the primary phone number with a sequence to cancel Call Waiting followed by the phone number, program the backup phone number **without** the Call Waiting cancel sequence. If the subscriber cancels Call Waiting service without notifying their alarm installing company, the control panel can still send reports using the backup number. Dialing a Call Waiting sequence on a non-Call Waiting line prevents the system from successfully dialing the central station receiver.

RPS Menu Location
Panel Wide Parameters > Phone and Phone Parameters > Phone 1, 2, 3, 4

Phone Format

Default: Modem4
Selections: Contact ID, Modem4
Contact ID When transmitting events over the GSM phone, only Contact ID is supported.
Modem4 The control panel sends expanded Modem4 Communication Format reports to the Central Station receiver.
This parameter sets the Central Station Receiver Format for transmission of reports. When using telephone reporting, event reports can be routed to a Central Station receiver using either Contact ID or Modem4 format. Modem4 reports identify points and passcode User ID codes at the receiver. When reporting point events, Modem4 also sends point text as programmed in Point Assignments. When using network reporting, event reports must be routed to a Conettix-compatible Central Station receiver using Modem4 format.
RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > Phone Format.

Additional Resources:
Point Assignments
DTMF Dialing
Default: Yes
Selections: Yes/No
Use DTMF (dual-tone multi-frequency) to dial the central station receiver phone number(s) for event reports, and/or RPS.
Yes: Dials the programmed phone number(s) using DTMF.
No: Pulse Dialing only
RPS Menu Location
Panel Wide Parameters > Phone and Phone Parameters > DTMF Dialing

Phone Supervision Time

Default: 0
Selections: 0, 10-240 (in 10 minute increments)
The control panel tests the primary phone line approximately nine times a minute and the secondary line once a minute. This prompt sets the amount of time the control panel continues to monitor a faulted phone line before initiating phone line trouble responses.
Keypads display [SERVC PH LINE #] to indicate which phone line failed. The keypad initiates a trouble tone if both Buzz On Fail and KP# Trouble Tone are set to 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.
IMPORTANT: To meet UL864 requirements, you must set this parameter to a non-zero value.
0: No phone line supervision.
10 - 240: Enter the number of seconds (in 10 second increments) to supervise the phone line. After a faulted phone line restores, it takes the same amount of time to initiate restoral responses.
Reference
Panel Wide Parameters > Phone and Phone Parameters > Phone Supervision Time

Alarm On Fail

Default: No
Selections: Yes or No
This parameter activates the Area 1 Burg Bell if the phone line fails.

IMPORTANT:
- Phone Supv Time must be programmed to use this parameter.
- The Alarm Bell output for Area 1 activates. All phone event messages report as Area 1 and/or the account number for Area 1.
- To meet UL864 requirements, set this parameter to **No**.

Yes: This option generates alarm responses when a phone line fails.
No: Phone failures report as trouble responses for Area 1 and/or the account number for Area 1.
Reference
Panel Wide Parameters > Phone and Phone Parameters > Alarm On Fail

Buzz On Fail

Default: No
Selections: Yes or No
This parameter activates the Trouble Tone if the phone line fails.

IMPORTANT:
- Phone Supv Time must be programmed to use this feature.
- Panel-wide trouble tones for individual keypads (based on their KP# 1 through 16) can be turned off by programming KP# Trouble Tone in keypad Parameters as NO.
- To meet UL864 requirements, set this parameter to **Yes**.

Yes: Generate panel-wide trouble tones and display [PHONE FAIL #] at keypads when a Phone Fail event occurs.
No: Do not generate trouble tones at keypads when a Phone Fail event occurs. [PHONE FAIL #] will still display.
RPS Menu Location
Panel Wide Parameters > Phone and Phone Parameters > Buzz on Fail

Two Phone Lines

Default: No
Selections: Yes or No
This program item is used when a D928 Dual Phone Line Module is connected to the control panel.

IMPORTANT:
- Program Phone Supv Time when using two phone lines.
- To meet UL 864 requirements, set this parameter to **Yes**.

Yes: D928 Dual Phone Line Module installed. The LEDs on the D928 light to indicate primary or secondary line trouble and COMM FAIL.
No: No D928 Dual Phone Line Module.
Reference
Panel Wide Parameters > Phone and Phone Parameters > Two Phone Lines

Expand Test Report

Default: No
Selections: Yes or No
This program item is used to add system event information to test reports. Test reports can be set up as manual or scheduled events in the Skeds section of the program.

Yes: Report events listed in routing group test reports are sent to the central station if they are off-normal.

No: Do not report off-normal conditions for the events listed in the routing group test reports at test time.

WARNING: When set to YES, this parameter will cause the Sked Functions Send Test Report and Send Off-Normal Test Report to be sent with extra information.

Reference
Panel Wide Parameters > Phone and Phone Parameters > Expand Test Report

3.2 Report Routing

Routing Overview

Report Routing lets you select full or partial groups of events to be reported up to four different destinations. Report Routing includes choosing which is the most important destination, (Route #), which events are reported to a single or multiple destination and if the events fail, which backup destination should be selected.

Called Party Disconnect
Telephone companies provide "called party disconnect" to allow the called party to terminate a call. The called party must go on hook (hang up) for a fixed interval before a dial tone is available for a new call. This interval varies with telephone company equipment. The control panel allows for "called party disconnect" by adding a 35 second "on hook" interval to the dial tone detect function. If the panel does not detect a dial tone in seven seconds, it puts the phone line on hook for 35 seconds to activate "called party disconnect," goes off hook and begins a seven-second dial tone detect. If no dial tone is detected, the panel dials the number anyway. Each time the number is dialed, the panel records this as an attempt. After 10 attempts the panel goes into Communications Failure and Comm Fail Route # is displayed on the Keypads.

Route # Groups, which has the highest priority?
To program a group, you first choose a Route # . The lower the Route # number, the higher priority that group will have (e.g., events reported for Route 1 have a higher priority than Route 2, 3 or 4 if each group has a message to send at the same time). This will become important when programming duplicate reports or choosing which events you want to ensure will report first regardless of the number of events that need to be reported to multiple groups. Remember, Route 1 group Primary Device will be the first destination that the panel will attempt to dial if an event in that group needs to be reported. If the panel is idle, any event generated for any group will initiate a dialing sequence.

Programming a Primary and Backup Destination
Each Route # has a Primary Device and Backup Device . In typical applications where two phone numbers are programmed, the Primary Device destination is the Phone # that the Route Group will attempt to dial first. If the Primary Device destination fails to connect to the central station receiver after two dialing attempts, then the Backup

Device destination will be dialed. In addition to this, the control panel can be programmed such that the Primary Device and/or the Backup Device can be an SDI device, such as a DX4020 Network Interface Module.

Programming a Duplicate report
To allow an event within a group to report to multiple groups, the event should be YES for each Route # available. For instance, programming Fire Alarms for Route Group 1 and Route Group 2 will result in the fire alarms first reporting to Route Group 1 followed by a duplicate report to Route Group 2.

Routing Destination Communication Failures
When the Primary Device fails to connect to the central station receiver after two attempts, the Backup Device phone number will be dialed. The central station will receive the original event with a COMM TROUBLE PHONE # =(1, 2, 3, or 4) message added. This event does not occur if there is no backup phone number. COMM RESTORE events are generated.
If the Primary Device is an SDI Path, the central station receives the original event with a COMM TROUBLE RG8 SDI## event modifier.

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

When all attempts to both the R# Primary Device and R# Backup Device fail, a COMM FAIL RG# event is generated. COMM RESTORE events are not generated.
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.

Message Prioritization Within a Route #
The 9000 Series Control Panels meet the digital reporting requirements for UL 864. Fire alarm events have the highest priority and are reported first for each group. The next highest priority events are in the following order, panic, duress, medical, intrusion alarm, supervisory and then all troubles and restorals.
IMPORTANT: To comply with NFPA and UL864, you must program Route 1 to report only Fire Alarm events to ensure the fastest reporting time.

Dialing Attempts
The primary device within a group will make six individual attempts to dial and the backup device will make four attempts to dial before initiating a local Comm Fail report. When only one destination is programmed, it will make 10 attempts. Each group takes approximately 10 minutes to go into Comm Fail.

Fire Reports

Default: Yes
Selections: Yes/No
IMPORTANT: To meet UL864 requirements for central station and remote station applications, enable fire reports.
Fire Alarm: Reports fire event.
Fire Restoral (After Alarm): Reports fire restoral from alarm.
Fire Missing: Reports missing fire point.
Fire Trouble: Reports fire trouble.
Fire Supervision: Reports fire supervision.
Fire Restoral (After Trouble): Reports fire restoral from trouble, missing, or supervisory.
Fire Cancel: Reports canceled fire alarm.
Fire Supervision Missing: Report fire supervisory missing.
Fire Supervision Restoral: Report fire supervisory restoral.
Reference
Panel Wide Parameters > Report Routing > Fire Reports

Gas Reports

Default: Yes
Selections: Yes/No
IMPORTANT: To meet UL864 requirements for central station and remote station applications, enable gas reports.
Gas Alarm: Reports gas event.
Gas Restoral from Alarm: Reports gas restoral from alarm.
Gas Missing: Reports missing gas point.
Gas Trouble: Reports gas trouble.
Gas Supervision: Reports gas supervision.
Gas Restoral from Trouble: Reports gas restoral from trouble, missing, or supervisory.
Gas Cancel: Reports canceled gas alarm.
Gas Supervision Missing: Report gas supervisory missing.
Gas Supervision Restoral: Report gas supervisory restoral.
Reference
Panel Wide Parameters > Report Routing > Gas Reports

Burglar Reports

Default: Yes
Selections: Yes/No
The Unverified Event is sent when a single point programming in Cross Point Group faults into an alarm condition, and then restores before the Cross Point Time elapses. This event encompasses both fire and non-fire points. It is not related to the Restart Time used for smoke detectors.
Restoral reports are not sent if the control panel is reset after a point is bypassed and then unbypassed. This is true for both fire and non-fire points.
Alarm Report: Report burglar alarm event.
Burg Restore (After Trouble): Reports non-fire restoral from trouble, missing, or supervisory.
Duress: Duress report.
Missing Alarm: Reports missing alarm point.

User Code Tamper: Reports user code tamper.
Trouble Report: Reports trouble event.
Missing Trouble: Reports missing trouble event.
Non-Fire Supervision: Reports non-fire supervision event.
Point Bus Fail: Reports point bus failure.
Point Bus Restoral: Reports restoral of point bus after failure.
Non-Fire Cancel: Reports canceled non-fire alarm.
Alarm Restore: Reports non-fire restoral from alarm.
Supervision Missing: Reports supervisory missing.
Unverified Event: Reports unverified events (includes fire & non-fire events).
Reference
Panel Wide Parameters > Report Routing > Burglar Reports

Personal Emergency Reports

Default: Yes
Selections: Yes/No
IMPORTANT: To meet UL864 requirements for central station and remote station applications, enable fire reports.
Medical Alarm: Reports medical alarm.
Medical Alarm Restoral: Reports restoral from medical alarm.
Silent / Hold-Up Alarm: Reports silent / hold-up alarm.
Silent / Hold-Up Alarm Restoral: Reports restoral from silent / hold-up alarm.
Panic Alarm: Reports panic alarm.
Panic Alarm Restoral: Reports panic alarm restoral.
Reference
Panel Wide Parameters > Report Routing > Personal Emergency Reports

User Reports

Default: Custom
- Point/Command Bypass: Yes
- Forced Point: Yes
- Point Opening: Yes
- Point Closing: Yes
- Was Force Armed: Yes
- Fail to Open: Yes
- Fail to Close: Yes
- Extend Close Time: Yes
- Opening Report: No
- Forced Close: No
- Closing Report: No
- Forced Close Part On Instant: No
- Forced Close Part On Delay: No
- Part On Instant: No
- Part On Delay: No
- Send User Text: Yes

Selections: Yes/No
Point/Command Bypass: Reports point bypass event.
Forced Point: Reports forced point event.
Point Opening: Reports point opening event.

Point Closing: Reports point closing event.
Was Force Armed: Reports point forced armed.
Fail To Open: Reports fail to open event.
Fail To Close: Reports fail to close event.
Extend Close Time: Reports extend close time event.
Opening Report: Reports opening events.
Forced Close: Reports point forced close event.
Closing Report: Reports closing events.
Forced Close Part On Instant: Reports forced close Part On instant event.
Forced Close Part On Delay: Reports forced close Part On delay event.
Part On Instant: Reports Part On instant event.
Part On Delay: Reports Part On delay event.
Send User Text: Reports user text.

RPS Menu Location

Panel Wide Parameters > Report Routing > User Reports

Test Reports

Default: Yes
Selections: Yes, No
Yes Enable reporting on all test events.
No Disable reporting on all test events.

This parameter enables or disables reporting on status' and tests. Use this parameter to manually select which test report functions to enable or disable reporting on.
Parameters within this route group are:

- Status Report
- Test Report

Reporting off-normal events as a status report following a test report, is required by some automation systems. Reporting off-normal events as a non-status report which follows a test report is required for other automation systems.
An off-normal event is any point which is missing, trouble, supervisory, or in alarm [as opposed to normal]. Also, points which have not been cleared at the keypad will report as off-normal.

RPS Menu Location

Panel Wide Parameters > Report Routing > Test Reports

Diagnostic Reports

Default: Custom
Selections: Yes, No
Yes Enables reporting for all diagnostic conditions.
No Disables reporting for all diagnostic conditions.
Custom This setting cannot be selected by the user. The field is populated automatically whenever some diagnostics reports are enabled and others are disabled.

This parameter enables or disables reporting on diagnostic results. Use this parameter to manually select which diagnostic functions to enable or disable reporting on.
The only time you should select specific reports from Diagnostic Reports is when you want to enable only some diagnostic reports but not all. Once changed, all Diagnostic

Reports selections made from that location appear as “Custom” in the corresponding Route Group.
If the off-normal state of the following events (indicated with a "[1]") still exists, they report when a test report is enabled and Expand Test Report is set to **Yes**.

Report	Selections	Report Description
SDI Device Failure[1]	**Yes**, No	SDI device failure.
SDI Device Restoral	**Yes**, No	Restoral of SDI device failure.
Watchdog Reset	**Yes**, No	Watchdog reset event.
Parameter Checksum Fail	**Yes**, No	Parameter checksum failure.
Reboot	**Yes**, No	Reboot event.
Phone Line Fail[1]	**Yes**, No	Failure of phone line.
Phone Line Restoral	**Yes**, No	Restoral of phone line after failure.
AC Failure[1,2]	**Yes**, No	Failure of AC power to control panel.
AC Restoral[2]	**Yes**, No	Restoral of AC power to control panel after failure.
Battery Missing[1,2]	**Yes**, No	Battery missing detection event.
Battery Low[1,2]	**Yes**, No	Low battery power.
Battery Restoral[2]	**Yes**, No	Restoral of battery power to control panel after Missing or Low event.
Route Comm Fail[1,3]	**Yes**, No	Failure to send report to specific route.
Rout Comm Restore	**Yes**, No	Restoral of communication to specific route after a failure.
Checksum Fail	**Yes**, No	Checksum fail event.
Network Fail	Yes, **No**	Failure of network.
Network Restoral	Yes, **No**	Restoral of network.
Network Condition	Yes, **No**	Condition of network.
RF Interference	**Yes**, No	Wireless Receiver interference
RF Interference Restoral	**Yes**, No	Wireless Receiver interference has been removed
Equipment Fail	Yes, **No**	Reports an occurrence of a SDI2 bus or module failure.
Equipment Fail Restoral	Yes, **No**	Reports restoral from an occurrence of a SDI2 bus or module failure.
Service Smoke Detector[1,2]	**Yes**, No	Reports an occurrence of a smoke detector failure.
Service Smoke Detector Restoral[2]	**Yes**, No	Reports restoral from an occurrence of a smoke detector failure.

Send Version Text	**Yes**, No	Send control panel and bootloader firmware versions with Reboot events.

[1] = Indicates an off-normal event.
[2] = To meet UL864 9th Edition requirements for Central Station and Remote Station applications, enable AC Fail, Battery Missing, Low Battery, Service Smoke Detector, Battery Restoral, AC Restoral reports and Service Smoke Detector Restoral.
[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.

Reference
Panel Wide Parameters > Report Routing > Diagnostic Reports

Output Reports

Default: Yes
Selections: Yes/No
When activating an on-board output using remote automation software, the control panel logs the resulting event as:
- Output 253 (Output A)
- Output 254 (Output B)
- Output 255 (Output C)

Sensor Reset: Reports sensor reset event.
Output Set: Reports output set event.
Output Reset: Reports output reset event.

Reference
Panel Wide Parameters > Report Routing > Output Reports

Auto Function Reports

Default: Yes
Selections: Yes/No
Sked Executed: Reports Sked executed event.
Sked Changed: Reports Sked changed event.
Fail to Execute: Reports a fail to execute event.

Reference
Panel Wide Parameters > Report Routing > Auto Function Reports

RPS Reports

Default: Yes
Selections: Yes/No
IMPORTANT: "RPS Access Fail" might indicate a wrong RPS passcode when communicating with the control panel, or a valid RPS session was abnormally terminated . "Remote Reset" indicates a Reset command was issued from RPS; "Bad Call to RPS" indicates that the control panel called RPS, but was unable to connect.
- Event Log Threshold. Reports Event log threshold reached.
- Event Log Overflow. Reports Log is full, old events will be overwritten.
- Parameters Changed. Reports RPS parameter change event.
- RPS Access OK. Reports successful RPS access event.
- RPS Access Fail. Reports failed access RPS event.
- Remote Reset. Reports remote reset event.

- Program Access OK. Reports successful local programming session event.
- Program Access Fail. Reports failed local programming session event.

RPS Menu Location
Panel Wide Parameters > Report Routing > RPS Reports

Point Reports

Default: Yes
Selections: Yes/No
- Service End: Reports service walk test end event.
- Fire Walk End: Reports fire walk end event.
- Walk Test End: Reports walk test end event for walk test and invisible walk test.
- Send Point Text: Reports point text. Point text is always sent when using NetCom applications.
- RF Low Battery Restore: Reports restoral from RF point low battery conditions.
- Bypass: Reports when a point has been removed from service.
- Bypass Restore: Reports when a point has been returned to service.

RPS Menu Location
Panel Wide Parameters > Report Routing > Point Reports

User Change Reports

Default: Yes
Selections: Yes/No
Date Changed: Reports date change event.
Time Changed: Reports time change event.
Delete User: Reports delete user code event.
User Code Change: Reports user passcode add or change event.
Area Watch: Reports area watch start and watch end.
Card/Keyfob Assigned: Reports card assigned or Keyfob assigned to user event.
Keyfob Removed: Reports when a keyfob assignment is removed from a user.
Change Level: Reports access control level change event.
Reference
Panel Wide Parameters > Report Routing > User Change Reports

Access Reports

Default: Yes
Selections: Yes/No
Access Granted*: Reports "access granted" event.
No Entry*: Reports "no entry" event.
Door Left Open: Reports "door left open" event.
Cycle Door: Reports "open door" event.
Door Unlocked: Reports "unlock door" event.
Door Secure: Reports "secure door" event.
Door Request*: Reports "request to enter" or "request to exit" event.
Door Locked: Reports "locked door" event.
* = "Access Granted," "No Entry," "Request to Enter" and "Request to Exit" events can be turned on or off by each individual D9210.
Reference
Panel Wide Parameters > Report Routing > Access Reports

3.3 Communicator

Communicator Overview

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:

Attempt #	Path Type
1	Primary Path Device
2	Primary Path Device
3	Backup Path Device
4	Backup Path Device
5	Primary Path Device
6	Backup Path Device
7	Primary Path Device
8	Backup Path Device
9	Primary Path Device
10	Backup Path Device

When only the primary path device is programmed, the control panel makes all ten attempts with that device. 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 categorize and individual events. Each group has a primary and a backup path device. The primary path device is the first (most important) destination used to reach the programmed route within this group. The backup path device is used if the primary path device fails.

IMPORTANT: By setting a Primary or Backup Path Device to an SDI or SDI2 communication device, the module automatically becomes supervised. Any loss of bus communication results in a SDI Fail system fault

Network Address Format

With the availability of the B426 (B420) it is now possible to enter a IPv4 or a fully qualified domain name in a Network Address field. The information below defines the proper format of the information that should be entered into the Network Address fields.

IP address (IPv4) Format

This is in ASCII decimal format.
xxx.xxx.xxx.xxx – eg 12.23.145.251 not C.17.91.FB. xxx = 0 to 255.

Fully Qualified Domain Name Format
The fully qualified domain name defines the exact address of a device in the Domain Name System hierarchy. This includes the unique hostname of the device and the subnet on which the device is located, separated by periods.
example: receiver01.your-alarm-company.com
Each label within the name must comply with RFC-921, "Domain Name System Implementation Schedule".
Only the alphabet (A-Z), digits (0-9), and the minus sign (-) are allowed in the text labels within the fully qualified domain name.
The period (.) is only allowed to delimit text labels that comprise the fully qualified domain name.
Before entering a fully qualified domain name, be sure the device being addressed has its name properly registered with the domain name system servers available to the Ethernet Communicator. This can be verified using a freely available ping tool.

Additional Information
Information on Hostnames and fully qualified Domain Name formats can be found on the "The Internet Engineering Task Force (IETF)" website http://www.ietf.org/

Primary Path Device

Default: No Device
Selections:

- No Device
- Phone 1
- SDI 88 Path 1
- SDI 92 Path 1
- SDI2 address 1 Path 1
- SDI2 address 2 Path 1
- Phone 2
- SDI 88 Path 2
- SDI 92 Path 2
- SDI2 address 1 Path 2
- SDI2 address 2 Path 2
- Phone 3
- SDI 88 Path 3
- SDI 92 Path 3
- SDI2 address 1 Path 3
- SDI2 address 2 Path 3
- Phone 4
- SDI 88 Path 4
- SDI 92 Path 4
- SDI2 address 1 Path 4
- SDI2 address 2 Path 4

IMPORTANT:
- To meet UL864 requirements for central station and remote station applications, program a primary device.
- You cannot select the same device option for both Primary and Backup Path Device within each route group.

Select the phone, SDI or SDI2 path that the control panel uses as its primary routing path to send reports to the central station receiver.
For more information on SDI and SDI2 paths, refer to Communicator -- Overview.

RPS Menu Location
Panel Wide Parameters > Communicator > Primary Path Device

Backup Path Device

Default: No Device
Selections:

- No Device
- Phone 1
- Phone 2
- Phone 3
- Phone 4
- SDI 88 Path 1
- SDI 88 Path 2
- SDI 88 Path 3
- SDI 88 Path 4
- SDI 92 Path 1
- SDI 92 Path 2
- SDI 92 Path 3
- SDI 92 Path 4
- SDI2 address 1 Path 1
- SDI2 address 1 Path 2
- SDI2 address 1 Path 3
- SDI2 address 1 Path 4
- SDI2 address 2 Path 1
- SDI2 address 2 Path 2
- SDI2 address 2 Path 3
- SDI2 address 2 Path 4

IMPORTANT:

- To meet UL864 requirements for central station and remote station applications, program a backup device.
- You cannot select the same device option for both Primary and Backup Path Device within each route group.

The backup device is used when the primary device fails to reach the programmed destination. Select the phone, SDI or SDI2 path that the control panel uses as its backup routing path to send reports to the central station receiver.
For more information on SDI or SDI2 paths, refer to Communicator Overview.
Reference Location:
Panel Wide Parameters > Communicator > Backup Path Device

RG Same Network Receiver

The Route Group 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 with different IP Addresses that can be accessed from more than one network such as on a LAN / WAN and over the Internet
- Both primary and backup paths use different poll rates, although it is not necessary.
- Either the primary or the backup path (not both) has a Communication Trouble condition.

RG Same Network Receiver Parameter Options
Default: Yes
Selections: Yes/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.
IMPORTANT: 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.
Reference Location:
Panel Wide Parameters > Communicator > RG Same Network Receiver

Time Synchronization

Default:
- Route Group 1: Yes
- Route Groups 2-4: No

Selections: Yes / No
This parameter enables the control panel to adjust its current time and date to bring the control panel into synchronization with the Central Station receiver. These options can only be configured from RPS.
The control panel provides a configuration option, Time Zone, which identifies the control panel's time offset from Universal Time Coordinate (UTC). This option is defaulted to the Eastern Time Zone. Time zones are provided in the drop-down menu. This configuration parameter is included in Time Zone. Also refer to Daylight Saving Time.
- Time Sync will not work when the Path Device is set to telephone.
- Time Sync can only be enabled in one route group at a time.
- Time Sync must be performed over a network connection.
- Time Sync is applicable to all route groups.

Off by 30 Minutes or Less:
The control panel adjusts its timekeeping to make up the difference. If the control panel's time is slow, the control panel counts seconds faster than once per second. If the control panel's time is fast, the control panel counts seconds slower than once per second. The modified counting of seconds remains in effect until the control panel time is in synchronization with the Central Station receiver time. Since every second occurs, there are no skips in time. No skeds scheduled to be run are skipped.
Off by More than 30 Minutes:
The control panel checks for a date change. If the day, month, or year has changed, the control panel's date is set to the new date. The control panel then sets its time to that of the Central Station receiver. Due to the skip in time, scheduled skeds might not run.
RPS Menu Location
Panel Wide Parameters > Communicator > Time Synchronization

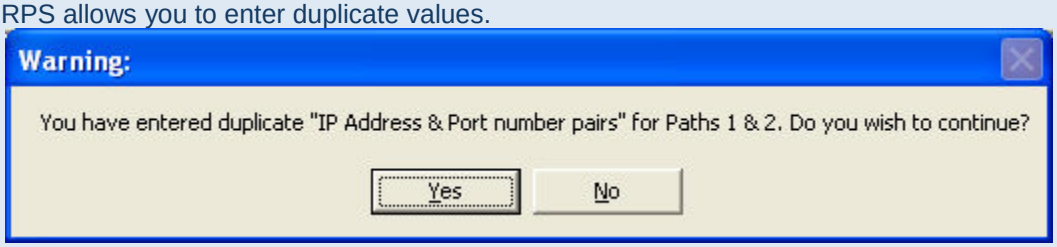
3.4 Enhanced Communications

Network Address (Paths 1 to 4)

Default: Blank
Selections: IPv4 Address (0.0.0.0 to 255.255.255.255) or Hostname (Up to 255 Characters)
There are up to four available Paths that events can be routed to. If an event (or group of events) are to be routed to an SDI Path, the number that is entered in Primary Device in the Routing section will determine which SDI Path will be used (as long as RG#, Primary SDI has been set to Yes in Routing as well).
If events are going to be routed to an IP Address (in a Private Local or Wide Area Network application), you will need to determine which Path will be used (Path 1 – Path 4) and then enter the appropriate IP Address for that Path.

IMPORTANT:

- If using IP Addresses as the communication means for UL 864 Commercial Fire applications, set Path # IP Address as necessary.
- Whenever the central station requests a change to the IP Address or Port Number configured in the control panel, the central station receiver must resynchronize the control panel's anti-replay/anti-substitution static key.
- When Port Number/IP Address pairs have duplicate values in a GV4 control panel, RPS shows the following warning message with Yes/No options. If you click **No**, RPS forces you to enter unique values for the **Port Number** and **IP Address** fields. If you click **Yes**, RPS allows you to enter duplicate values.



- Refer to Network Address Format for more information.

Reference
Panel Wide Parameters > Enhanced Communications > Network Address (Paths 1 to 4)

Port Number (Paths 1 to 4)

Default: 7700
Selections: 1 to 65,535 (increments of 1)
Assign a unique port number for each path used to the central station's Network address.

IMPORTANT:

- When upgrading from a G-series control panel that does not support network communication to a GV4 control panel account, RPS forces the default to **7700**.
- Whenever the central station requests a change to the Network Address or Port Number configured in the control panel, the central station receiver must resynchronize the control panel's anti-replay/anti-substitution static key.

Reference
Panel Wide Parameters > Enhanced Communications > Port Number (Paths 1 to 4)

Receiver Supervision Time

Default: 1 Hour
Selections:

200 Seconds	UL 1610
300 Seconds	NFPA 72 2010
1 Hour	NFPA 72 2013
4 Hours	Medium Security
24 Hours	Daily
25 Hours	
90 Seconds	High Security
No Polling	
95-195, 205-1275 Seconds	Selections available in 5 second intervals. Poll Rate, ACK Wait and Retry Count fields are automatically populated based on the selection and cannot be changed.
2, 3, 5-24, 26-255 hours	Poll Rate, ACK Wait and Retry Count fields are automatically populated based on the selection and cannot be changed.
Custom	Custom is the only selection that will allow the user to manually select values for Poll Rate, ACK Wait, and Retry Count. When Custom is selected for the first time, the default value for Poll Rate, ACK Wait and Retry Count is zero. After the user modifies the values, these values remain each time Custom is selected until new values are set.

Cellular Settings for High Supervision Sites (Faster than 1 hour supervision)
The vast majority of cellular installations can be supervised at settings of 4 hours to 24 hours, but for high security and fire listed installations where cellular is the primary or sole communication path and supervision rates are 1 hour or less you should consider changing the following cellular parameters in the panel or cellular device bus module:

Reporting Delay for Low Signal & Reporting Delay for No Towers: 200 seconds. For some listed high security installations, low cellular signal is required be treated like a wire cut and reported within 200 seconds. This will increase sensitivity to cellular tower maintenance windows and other environmental conditions, so we recommend leaving the default settings for non-listed installations.

Reporting Delay for Single Tower: 600 seconds. For sole path cellular sites with supervision at 5 minutes or less where only one cell tower is available, maintenance (generally 1-5 minutes in the early morning hours) or changes in environmental conditions may cause communication troubles to be reported. To detect and report single tower conditions at cellular sites using a plug-in cellular module in the panel or on GV4 version 2+ or B Series SDI2 bus, enable Single Tower trouble reporting. The number of towers available can be viewed in the B450 module's USB menu or on keypads of SDI2 control panels with version 2+.

NOTICE: For SDI and Option bus installations of a cellular module, trouble conditions such as Low Signal and Single Tower result in the device going missing from the bus when the delay timer is reached.

RPS Menu Location
Panel Wide Parameters > Enhanced Communication > Receiver Supervision Time

IMPORTANT CELLULAR SERVICE INFORMATION
To avoid monthly overages, Bosch offers service plans that align with the common applications for cellular connectivity on alarm panels. To optimize data used for supervision, refer to the Recommended supervision configuration table.

Poll Rate (Paths 1 to 4)

Default: 3240
Selections: 0, 5 to 65535 (seconds)
Each SDI path can be configured to send a heartbeat poll to the central station for supervision purposes. This ensures the integrity of the connection at all times.

IMPORTANT:
- If using IP addresses as the communication means for UL864 9th edition commercial fire applications, program this parameter as necessary.
- When sending reports to a central station receiver over a network path, set this parameter to a non-zero value. Failure to program a value into this parameter could prevent a failed network communication path from restoring to normal.
- If the control panel is programmed to send a heartbeat poll to the central station, a rate of 75 seconds maintains the virtual link in most network configurations. Decreasing the value for this parameter increases the amount of idle communication between the SDI device and the central station receiver. Increased idle communication between the control panel and receiver decreases the control panel's event reporting efficiency.
- The control panel readjusts the heartbeat poll rate temporarily to less than 300 seconds to 300 seconds when online with RPS. The poll rate returns to the programmed value after the RPS session ends.

The value entered in this parameter is the interval (in seconds) at which the control panel sends a heartbeat poll to the central station receiver. The value entered in ACK Wait Time (Paths 1 to 4) 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's retry count entry is greater than zero. If so, the control panel retries the number of times entered in Retry Count (Paths 1 to 4) to send the heartbeat poll before declaring the path failed and generating a COMM FAIL SDI ## (Path 1 = SDI 88, Path 2 = SDI 89, Path 3 = SDI 90, Path 4 = SDI 91) event.
Poll Rate (Paths 1 to 4), ACK Wait Time (Paths 1 to 4), and Retry Count (Paths 1 to 4) 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).

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

If this parameter 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 Comm Fail for more information.

Heartbeat Example:

- Poll Rate (Paths 1 to 4) = 120 seconds
- ACK Wait Time (Paths 1 to 4) = 10 seconds
- Retry Count (Paths 1 to 4) = 2

When the control panel first powers up, the first heartbeat poll for Path 1 is sent and acknowledged in 1 second. 120 seconds after the first heartbeat poll is sent, the second heartbeat poll for Path 1 is sent to the central station receiver.

Retry Count Example:

An acknowledgement of the heartbeat was not received within 10 seconds. The control panel sends the next heartbeat poll after the first 10-second ACK wait period expires. If the central station does not acknowledge this heartbeat poll, the control panel continues to resend. When the resend count is reached, the control panel declares this path as failed and generates the Comm Fail ## event. The control panel continues to re-send the heartbeat poll every 10 seconds until it receives an acknowledgement, even after declaring a Comm Fail.

When the control panel receives acknowledgement from the central station, the control panel returns to the normal poll rate.

If more than one SDI path is used, the control panel handles them on a successive basis. For example, if acknowledgement from SDI Path 1 is not received within 10 seconds (based on the above 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 resend the heartbeat poll.

Entries are made in 1-second increments.

- 5 minutes = 300 seconds
- 1 hour = 3600 seconds
- 12 hours = 43,200 seconds
- 18 hours = 64,800 seconds

IMPORTANT: If heartbeat polls are enabled to send by an SDI path, and ACK Wait Time (Paths 1 to 4) is exceeded, a COMM FAIL ## event occurs. When this condition occurs, all events routed to this path go immediately to the backup path.

0: Disables the ‘heartbeat’ poll.

5 to 65534: Enables the poll rate for the amount of time programmed here (in seconds).

65535: The 'heartbeat' poll occurs once a day.

RPS Menu Location

Panel Wide Parameters > Enhanced Communications > Poll Rate (Paths 1 to 4)

IMPORTANT CELLULAR SERVICE INFORMATION
To avoid monthly overages, Bosch offers service plans that align with the common applications for cellular connectivity on alarm panels. To optimize data used for supervision, refer to the Recommended supervision configuration table.

ACK Wait Time (Paths 1 to 4)

Default: 60
Selections: 5 to 65535 (seconds)
This item determines how long the control panel will wait for an acknowledgement from the central station after a heartbeat event (poll) or an actual event has been transmitted. This prompt is only applicable to SDI transmitted events. Entries are made in one second increments.
5 to 65,535: The control panel will wait this amount of time to receive an acknowledgement from the central station.
RPS Menu Location
Panel Wide Parameters > Enhanced Communications > ACK Wait Time (Paths 1 to 4)

IMPORTANT CELLULAR SERVICE INFORMATION
To avoid monthly overages, Bosch offers service plans that align with the common applications for cellular connectivity on alarm panels. To optimize data used for supervision, refer to the Recommended supervision configuration table.

Retry Count (Paths 1 to 4)

Default: 5
Selections: 0 to 255
This item determines how many times the control panel will re-send the heartbeat event before declaring a Path Failure and generating a COMM FAIL RG8 SDI ### event where SDI ## is defined by the following device and path combinations.

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

IMPORTANT: To meet UL864 requirements, set this parameter as necessary if using IP addresses as the primary communication method.
- 0: `COMM FAIL RG8 SDI ###` events are not generated.
- 1 to 255: `COMM FAIL RG# SDI ###` events are generated after the number of retries are reached for a given SDI Path.

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > Retry Count (Paths 1 to 4)

AES Key Size

Default: No Encryption
Selections: No Encryption, 128, 192, 256
This parameter is used to select the AES key size.
RPS Menu Location
Panel Wide Parameters > Enhanced Communications > AES Key Size

AES Encryption Key

Default: <Default>
Selections: Thirty-two hexadecimal characters represented by an ID (01 to 100).
This parameter allows each receiver path to be configured with a unique AES encryption key.
The AES Encryption Key is based on AES Key Size. For the encryption key configuration, only Key ID & Name is displayed.
By default RPS sets the AES Key string to <Default>. RPS validates if two or more network paths have the same network address. If yes, then RPS notifies the user to use the same encryption key for those network paths.
IMPORTANT
- When using encryption with a GV4 panel, any DX4020 or ITS - DX4020G module on the SDI bus must have its encryption feature set to NO. The panel does the encryption instead of the module.
- When configuring the B420 or the B426 using the web interface, encryption must be set to NO. The panel now controls the encryption.
  Setting encryption to YES will prevent the panel from sending reports.

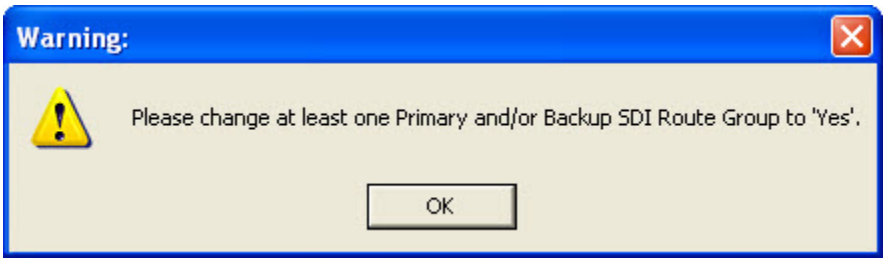
RPS Menu Location
Panel Wide Parameters > Enhanced Communications > AES Encryption Key

Additional resources:
AES key strings are configured in Config >> System >> Encryption Key Tab

3.5 SDI RPS/Enhanced Communication

Enable Enhanced Communication

Default: Yes
Selections: Yes/No
If Yes is selected this indicates that the desired operation includes an IP path as a communications channel. In order to select Yes as a configuration option one of the four Primary or Backup SDI Route groups should be set to an SDI or SDI2 communicator path. If a Primary or Backup Route group is not set properly the following dialog will be displayed. *NOTE: For setting Route Groups reference Panel Wide Parameters > Communicator*



If set to No then the intended operation would be that event routing would occur via a PSTN connection.

RPS Menu Location

Panel Wide Parameters > SDI RPS / Enhanced Communications > Enable Enhanced Communication.

Answer RPS Over Network?

Default: Yes

Selections: Yes/No

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

This parameter can be momentarily disabled by selecting ALLOW ANSWER through MENU 34 (Remote Programming) menu.

IMPORTANT: If the reset pin is in the locked position, local RPS programming is still allowed even if this prompt is set to **No**.

Yes: Enable automatic answer of RPS initiated sessions over the network.

No: Do not automatically answer RPS initiated sessions over the network.

Reference

Panel Wide Parameters > SDI RPS / Enhanced Communications > Answer RPS Over Network

RPS Address Verification

Default: No

Selections: Yes/No

When enabled, this parameter verifies that RPS connects to the control panel from a known IP address. This verification can be temporarily disabled by selecting ALLOW ANSWER in the MENU 34 menu.

Yes: Verifies that the incoming RPS IP address matches the address entered in RPS Network Address.

No: Allow RPS to connect to the control panel from any IP address. No verification is performed.

Reference

Panel Wide Parameters > SDI RPS / Enhanced Communications > RPS Address Verification

RPS Network Address

Default: blank

Selections: IPv4 address or Hostname

Enter the IP address or hostname for RPS.

Be sure to contact your network administrator to find out which IP Address or hostname your RPS computer is connected to.

Network Address Format

Reference

Panel Wide Parameters > SDI RPS / Enhanced Communications > RPS Network Adddress

RPS Port Number

Default: 7750
Selections: 1 – 65,535
This parameter is used as the destination UDP port for control panel-initiated RPS network sessions.
Reference
Panel Wide Parameters > SDI RPS / Enhanced Communications > RPS Port Number

3.6 Power Supervision

AC Fail Time

Default: 01:00
Selections: 00:01 to 90:00 (Minutes:Seconds)
Enter the amount of time that the AC power must be off before the control panel sends an AC Failure report.
IMPORTANT: To meet UL864, the following conditions must be met:
- Set AC Tag Along to **Yes**.
- Set AC Fail/Restoral Report to **No**.
- Enter an odd-numbered value in this parameter within the range of 61:00 to 89:00

Reference
Panel Wide Parameters > Power Supervision > AC Fail Time

Resend AC Fail

Default: No Report
Selections:
- No Report
- After 6 Hours
- After 12 Hours

Select the time interval that must pass without the AC failure condition being restored before the control panel resends the AC Failure report to the central station.
Reference
Panel Wide Parameters > Power Supervision > Resend AC Fail

AC Fail Display

Default: 60
Selections: 10 to 300 seconds (increments of 5)
Enter the amount of time in seconds the system waits before sounding a local AC Failure annunciation.
IMPORTANT:
- To comply with UL standards, the entry for this parameter should not exceed 200 seconds.
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **60 seconds**.

Reference
Panel Wide Parameters > Power Supervision > AC Fail Display

AC Fail/Restoral Report

Default: No
Selections: Yes/No
AC Power Supervision reports are sent to the central station at the time programmed for *AC Fail Time*.
IMPORTANT: To comply with NFPA standards and UL 864 requirements for Commercial Fire Systems, set this parameter to No, and set AC Tag Along to Yes.
Yes: Send AC Fail and AC Restoral reports.
No: Do not send AC Fail and AC Restoral reports.
Reference
Panel Wide Parameters > Power Supervision > AC Fail/Restoral Report

AC Tag Along

Default: Yes
Selections: Yes/No
Send AC reports only if any other event occurs while AC is off-normal.
IMPORTANT: AC Tag along is required for NFPA and UL 864 Commercial Fire Systems. Set AC Fail/Res Report to No if this parameter is set to Yes.
Yes: Send AC messages as tag along events.
No: Do not send AC messages as tag along events.
Reference
Panel Wide Parameters > Power Supervision > AC Tag Along

AC/Battery Buzz

Default: No
Selections: Yes/No
Initiate a panel-wide trouble tone at keypads when AC fails or battery is low or missing. This parameter does not prevent SERVC AC FAIL or SERVC BATT LOW displays.
IMPORTANT:
- To comply with NFPA standards and UL 864 requirements for commercial fire systems, set this parameter to Yes.
- Panel-wide trouble tones for individual keypads (based on their KP# 1 through 16) can be turned off by setting KP# Trouble Tone to No.

Yes: Initiate panel-wide trouble tone at all keypads.
No: Do not Initiate panel-wide trouble tone at keypads.
Reference
Panel Wide Parameters > Power Supervision > AC/Battery Buzz

Battery Fail/Restoral Report

Default: Yes
Selections: Yes/No
This parameter determines if a report is sent if the battery is low or missing.
The battery must be discharged below 12.1VDC for 16 seconds before the control panel responds to a low battery. It takes between 10 and 60 seconds for a missing battery to be detected.
IMPORTANT: To comply with NFPA standards and UL 864 requirements for commercial fire systems, set this parameter to Yes.

Yes: Battery failure and restoral reports are sent to the central station. They are routed to the telephone number programmed for *Power/Phone* events.
Modem reports: Missing or shorted `BATTERY MISSING`; discharged below 12.1VDC `BATTERY LOW`
Contact ID reports: Missing or shorted `BATTERY MISSING/DEAD`; discharged below 12.1VDC `LOW SYSTEM BATTERY`
No: Battery failure and restoral reports are NOT sent to the central station.
Reference
Panel Wide Parameters > Power Supervision > Battery Fail/Restoral Report

3.7 RPS Parameters

RPS Passcode

Default: 999999
Selections: 6-24 characters
Enter 6-24 characters. Do not use SPACE in the passcode.
The RPS passcode verifies that the RPS operator has valid access to connect to the control panel.
Reference
Panel Wide Parameters > RPS Parameters > RPS Passcode

Log % Full

Default: 0
Selections: 0 to 99
This parameter determines how full the memory log should be before initiating a call to RPS at the central station. This allows the central station to call the control panel and copy the memory log before messages could 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 central station receiver.
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.
IMPORTANT: The log overflow event is not sent to the central station unless Expand Test Rpt is set to Yes.
To configure RPS and the control panel to use the Contact RPS if Log % Full feature, refer to FAQs#Contact_RPS_Log_Full in the FAQs topic.
Reference
Panel Wide Parameters > RPS Parameters > Log % Full

Contact RPS if Log % Full

Default: No
Selections: Yes/No
When this parameter is set to **Yes**, the control panel automatically calls RPS when the "Log % Full" limit is reached.
To configure RPS and the control panel to use the Contact RPS if Log % Full feature, refer to FAQs#Contact_RPS_Log_Full in the FAQs topic.
Reference
Panel Wide Parameters > RPS Parameters > Contact RPS if Log % Full

RPS Call Back

Default: No
Selections: Yes/No
Using this function allows the control panel, after it has verified the RPS passcode, to provide an additional level of security by hanging up and dialing the RPS phone number to call RPS at the central station prior to allowing any upload or download.
IMPORTANT: When using the RPS Callback function, enter a "C" as the last digit in the RPS phone number if DTMF dialing is used.
Yes: When the control panel hears the proper RPS passcode, it hangs up the phone, seizes the phone line, then dials the programmed RPS phone number (see RPS Ph). This ensures that only the control panel communicates with the RPS PC connected to the dialed phone number.
No: The RPS session is initiated immediately; no call back is required. The control panel engages in RPS sessions when called from any phone number and a proper RPS passcode is identified.
Reference
Panel Wide Parameters > RPS Parameters > RPS Call Back

RPS Line Monitor

Default: Yes
Selections: Yes/No
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 has answered the phone. You must set Answer Armed and/or Answer Disarmed, and the control panel must be in the proper armed state.
IMPORTANT:
- If RPS Call Back is set to Yes, the control panel hangs up the phone after the RPS tone and a proper RPS passcode is identified, then it calls the RPS phone number.
- Set this parameter to No if it causes false seizures of the phone line, or if you are not using RPS. This would indicate that a device using the same frequency tone is also using the phone line to which the control panel is connected.

Yes: Allow the control panel to communicate with RPS after the answering machine has answered the phone.
No: This item should be set to No if the control panel is not sharing the phone line with an answering machine.
Reference
Panel Wide Parameters > RPS Parameters > RPS Line Monitor

Answer Armed

Default: 7
Selections: 0 to 15
Set the telephone ring counter to answer when all areas are All On. If any area in the control panel is Part On or disarmed, the Answer Disarmed ring counter is used.
IMPORTANT: RPS considers Part On as a disarmed state.
0 (zero): No answer
1 to 15: The control panel answers the phone after the specified number of rings when all areas are All On.
Reference
Panel Wide Parameters > RPS Parameters > Answer Armed

Answer Disarmed

Default: 7
Selections: 0 to 15
Set the telephone ring counter to answer when any area is in a Part On or disarmed state.
IMPORTANT: RPS considers Part On as a disarmed state.
0 (zero): No answer
1 to 15: The control panel answers the phone after the specified number of rings when all areas are All On.
Reference
Panel Wide Parameters > RPS Parameters > Answer Disarmed

RPS Phone

Default: Blank
Selections: Up to 24 characters
Enter in this parameter the phone number the control panel dials to contact RPS. The control panel dials the programmed number using Phone #5 (RPS Phone #) as a result of the following events:
- Log % Full threshold is achieved
- The control panel is contacted by RPS and RPS Call Back is programmed Yes
- MENU 34 is initiated and the user selects CALL RPS option

If this parameter is left empty (blank), the control panel does not dial a phone number for RPS.
IMPORTANT:
- See Phone 1,2,3,4 when programming this parameter.
- When an RPS phone number is entered, the user can call RPS by pressing MENU 34, then select Call via Phone. When performing this function, only one attempt is made to contact RPS.
- If you enter a value from 1 to 99 in Log % Full and you enter an RPS phone number in this parameter, the control panel dials the RPS phone number when the log threshold is reached.

Reference
Panel Wide Parameters > RPS Parameters > RPS Phone #

RPS Modem Speed

Default: 1200
Selections:
– 300
– 1200
– 2400
Select the baud rate for RPS-to-control panel-communication when using a PSTN connection.
Reference
Panel Wide Parameters > RPS Parameters > RPS Modem Speed

3.8 Miscellaneous

Duress Type

Default: 0
Selections: 1, 2, or 3
This parameter determines whether users add one (+1) or two (+2) to the last digit of the passcode. To activate a duress alarm, the user increases the value of the last digit of their passcode when entering it at the keypad.

IMPORTANT:
- Duress is enabled or disabled by area in *Area Parameters* and by user in Authority Levels.
- The duress alarm is activated when a user enters the duress combination followed by the termination keys (ESC or ENT).
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to **3**. See SIA CP-01 Verification for more information.

Option	Description
0	Disabled.
1	Increase the last digit by 1 to generate an alarm. For example: • If the passcode is 612**3**, 612**4** activates a duress alarm. • 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. • 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 last digit of the passcode is **8**, a duress alarm occurs when the user enters **0** as the last digit of the passcode. • 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 user passcode entered with Send Duress set to **Yes.**

Reference
Panel Wide Parameters > Miscellaneous > Duress Type

Cancel Reports

Default: Yes
Selections: Yes/No
Use this parameter to determine whether or not Cancel, Fire Cancel and Gas Cancel reports are sent.
A Cancel, Fire Cancel and Gas Cancel report is created when a passcode is entered to silence an Alarm Bell, Fire Bell or Gas Bell before the bell time expires.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. See SIA CP-01 Verification for more information.
Yes: Send cancel reports according to routing.
No: Do not send cancel reports.
Reference
Panel Wide Parameters > Miscellaneous > Cancel Reports

Call for Service Text

Default: Contact your dealer
Selections: Enter up to 32 characters.
This parameter allows the user to customize the Call for Service message that is displayed at keypads.
Enter up to 32 characters of text.
- SDI2 keypads display the first 20 characters. If more than 20 characters are used, the text scrolls across the display one time. To scroll the text again, press [ESC].
- Spaces before, after and within a string of text are treated as text and are included in the 32 character limit.
- On SDI keypads, only the first 16 characters display.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Call for Service Text

On-site Authorization for Firmware Update

Default: No
Selections: Yes / No
This parameter is set to **Yes** if the installation requires that authorized personnel on site enter the authorization code at one of the keypads at the designated time during the remote firmware update process.
If this parameter is set to **No**, then there is no authorization required on site. If authorization is required, you can modify the authority level required for the authorized user (refer to Remote Firmware Update).
NOTE: It is recommend that a full system test be performed whenever firmware is updated locally or remotely.
Reference
Panel Wide Parameters > Miscellaneous > On-site Authorization for Firmware Update

Fire Summary Sustain

Default: Yes
Selections: Yes or No
The purpose of the Fire Summary Sustain configuration option is to provide a fire or gas alarm output to keep fire strobes active after the fire or gas bell has stopped sounding.
Summary Fire Output – When Fire Summary Sustain is set to **Yes**, the Summary Fire Output turns on when the first fire alarm is detected. The output remains active until all fire alarms have been acknowledged, returned to normal, and removed from the keypad display. Because acknowledging a fire alarm silences the fire alarm bell, the output remains active after the bell has been silenced. When Fire Summary Sustain is set to **No**, the Summary Fire Output turns on when the first fire alarm is detected and turns off when all fire alarm points have returned to normal. Note that the Summary Fire Output might turn off prior to the fire alarm bell silencing. The Fire Summary Sustain settings perform an identical function for the Summary Gas Output.
Summary Supervisory Fire Output – Alarms and strobes are not typically associated with a supervisory fire event, yet the Fire Summary Sustain option affects the Summary Supervisory Fire Output because Fire Supervisory conditions are latching. When Fire Summary Sustain is set to **Yes**, the Summary Supervisory Fire Output turns on when the first fire supervisory is detected. The output remains active until all fire supervisory conditions have been acknowledged, returned to normal, and removed from the keypad display. When Fire Summary Sustain is set to **No**, the Summary Supervisory Fire Output turns on when the first fire supervisory is detected and turns off when all fire supervisory points have returned to normal. The Fire Summary Sustain settings perform an identical function for the Summary Supervisory Gas Output.
Summary Fire Trouble Output – Because fire troubles are self-restoring, the Fire Summary Sustain option has no effect on the Summary Fire Trouble Output. The Summary Fire Trouble Output turns on when the first fire trouble is reported. The output remains active until all fire trouble conditions have returned to normal. No user action at a keypad is required to clear the Summary Fire Trouble Output. The Fire Summary Sustain settings perform an identical function for the Summary Trouble Gas Output.
Yes: Forces the Summary Fire and Summary Gas output to remain on after the Alarm Silence command.
No: Allows Summary Fire and Summary Gas output to activate when a corresponding point in the system goes into alarm. This output provides a steady output until all fire points in the system are returned to normal.
Reference
Miscellaneous > Fire Summary Sustain

Fire Supervision Event Type

Default: 2 (Fire Supervision Restoral)
Selections:
– 0 (Fire Trouble Restoral)
– 1 (Fire Alarm Restoral)
– 2 (Fire Supervision Restoral)
This item determines how the control panel transmits a Fire Supervision Restoral event.
0 (Fire Trouble Restoral): The panel transmits a `FIRE TROUBLE RESTORE` when a Fire Supervision point restores to normal.
1 (Fire Alarm Restoral): The panel transmits a `FIRE ALARM RESTORE` when a Fire Supervision point restores to normal.
2 (Fire Supervision Restoral): The panel transmits a `FIRE SUPERVISION RESTORE` when a Fire Supervision point restores to normal.
Reference
Miscellaneous > Fire Supervision Event Type

Fire Trouble Resound

Default: No Fire Trouble Resound
Selections:
– No Fire Trouble Resound
– Fire Trouble Resound @ 12:00 PM
– Fire Trouble Resound @ 12:00 AM
This item determines if a fire trouble condition, although previously acknowledged and silenced at a keypad, will automatically resound the fire trouble tone at 12:00 P.M., 12:00 A.M., or not at all if the point is still in an off-normal state. Additionally, when this parameter is set to resound, user authentication will be required to silence troubles. A user's pass code must have an authority level of 1 or greater in an area to silence troubles.
No Fire Trouble Resound: Keypads will not re-sound the fire trouble tone.
Fire Trouble Resound @ 12:00 PM: Keypads will re-sound the fire trouble tone at 12:00 P.M. (noon) if any fire point that falls within the scope of a keypad is in an off-normal state.
Fire Trouble Resound @ 12:00 AM: Keypads will re-sound the fire trouble tone at 12:00 A.M. (midnight) if any fire point that falls within the scope of a keypad is in an off-normal state.
Reference
Miscellaneous > Fire Trouble Resound

Early Ambush Time

Default: 10
Selections: 5 to 30 (1-minute increments)
Enter the amount of time allowed for the user to enter a second passcode at the keypad when Early Ambush is set to Yes.
IMPORTANT: If a second passcode is not entered before the Early Ambush Time ends, a Duress is generated based on the first user passcode.
Reference
Miscellaneous > Early Ambush Time

Second Ambush Code

Default: Unique
Selections: Unique, Any
This parameter determines whether the same passcode can be used to start and end the Early Ambush process.
Unique: The passcode used to end the Early Ambush Time must be different from the passcode used to disarm the area.
Any: The Early Ambush Time can be stopped using a different passcode, or the same passcode used to disarm the area.
Reference
Miscellaneous > Second Ambush Code

Abort Window

Default: 30 sec
Selections: 15 to 45 sec (1-sec increments)
Enter the number of sec the control panel delays sending an alarm event to the central station from a point with the Alarm Event Abort feature enabled.
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 (see Abort Display).
When an abort alarm timer starts, it does not stop until an alarm silence operation is performed, or the time expires.

IMPORTANT:
- This feature does not apply to fire alarms or invisible point alarms.
- To meet UL requirements, the combined Entry Delay and Abort Window time must not exceed 60 sec.
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **15 sec**.
- For SIA CP-01 Compliance, Abort Window is a required parameter.

Reference
Miscellaneous > Abort Window

Passcode Length

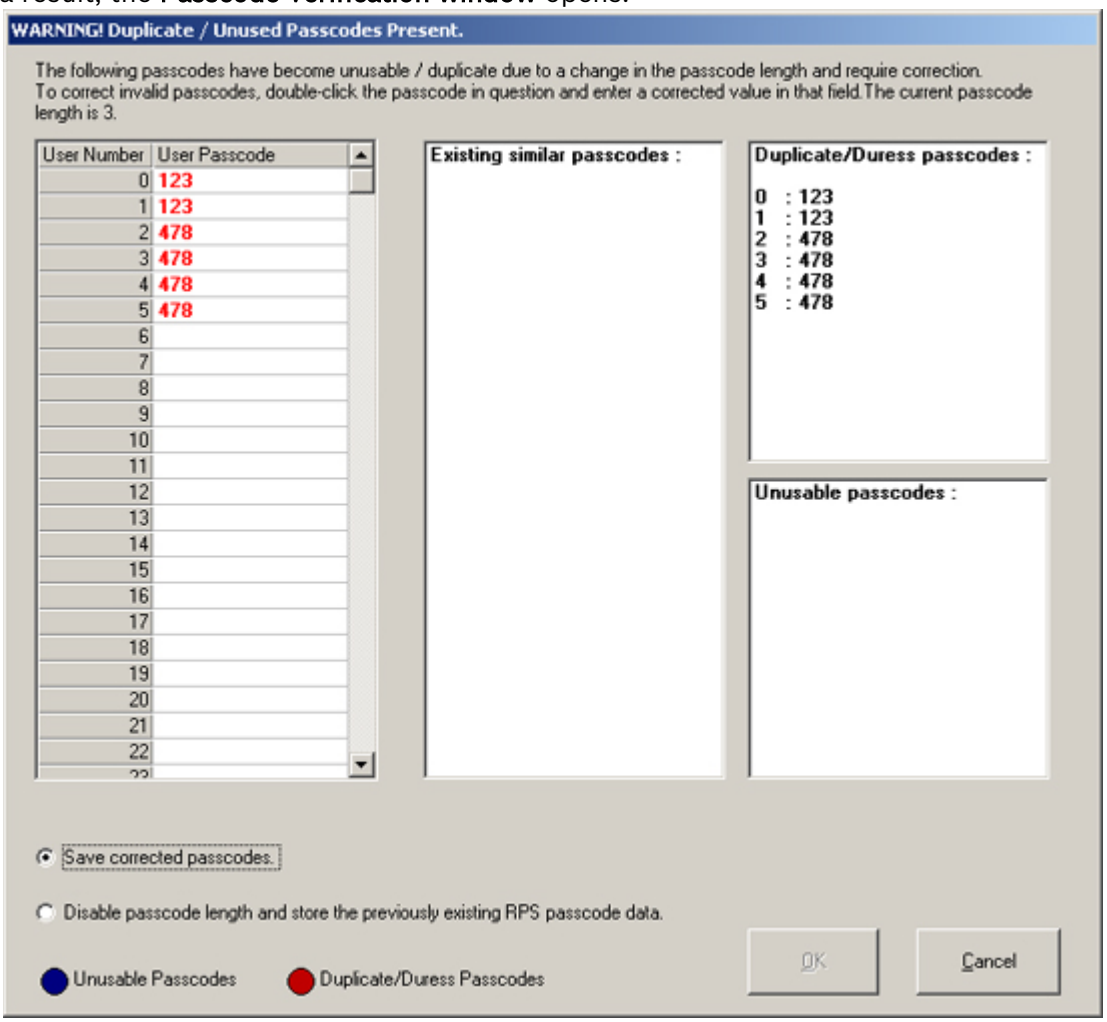
Default: Disabled
Selections:
- Disabled
- 3, 4, 5, or 6 digits

Select the number of digits allowed in all passcodes.

IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter between 3 and 6 digits. See SIA CP-01 Verification for more information.

Changing a Passcode

If the passcode length is changed and duplicate or unusable passcodes are created as a result, the **Passcode Verification window** opens.



If a passcode is identified as a duplicate passcode, it is marked in **bold red**.

If a passcode is identified as unusable (length is under or over the value entered in this parameter), it is marked in **bold blue**.

To change a passcode:

1 Click the appropriate cell in the User Passcode column to select the passcode.
2 Press the [Backspace] key on your keyboard to clear the cell.
3 Enter the new passcode.

There are two option buttons that control how this parameter handles passcode entries:

- **Save corrected passcodes:** This option is selected by default. All passcodes marked as duplicate or unusable must be fixed before you click **OK** to save the passcode corrections.
- **Disable passcode length and store the data in this account:** This option disables the Passcode Length parameter and allows you to save passcodes of varying lengths in the RPS account.

IMPORTANT: When the second option (**Disable passcode length and store the data in this account**) is selected, RPS sets the SIA CP-01 Verification parameter to **No** and then

notifies the RPS operator with a Yes/No dialog for each of the following scenarios. Select **Yes** or **No** as appropriate.

- **Change in Passcode Length parameter:** RPS displays the following message dialog: "This operation will cause the Passcode Length to be disabled, SIA CP-01 Verification parameter will be set to No and previously existing RPS passcode data will be stored. Are you sure you want to continue?"
- **Passcode Length Changes via the SIA CP-01 Verification parameter:** RPs displays the following message dialog: "This operation will cause the Passcode Length to be disabled, all other parameters previously updated in the SIA Compliance Warning window will be saved, SIA CP-01 Verification parameter will be set to No and previously existing RPS passcode data will be stored. Are you sure you want to continue?"
- **Incorrect Passcodes:** RPS displays the following message dialog: "This operation will cause the Passcode Length to be disabled, SIA CP-01 Verification parameter will be set to No and the panel's passcode data will be stored. Are you sure you want to continue?"
- **Passcode Length Change during Send/Receive:** RPS displays the following message dialog: "This operation will cause the Passcode Length to be disabled, all other parameters previously updated in the SIA Compliance Warning window will be saved, SIA CP-01 Verification parameter will be set to No and the panel's passcode data will be stored. Are you sure you want to continue? "

Similar and Duplicate Passcodes

You must change your entry to one that does not match or resemble an existing passcode.

- **Similar Passcodes:** If the passcode you enter resembles another existing passcode, the existing passcode appears in the Existing Similar Passcodes field.
- **Duplicate Passcodes:** If you enter a passcode that matches an existing passcode, the existing passcodes appear in the Duplicate/Duress Passcodes field. Passcode matches are based on duplicate entries with the length set to the lowest value that complies with SIA CP-01 (3).

For example, if you enter "478123" as a passcode for User 2, and "478321" as a passcode for User 3, and you set Passcode Length to three digits, the passcodes for Users 2 and 3 appear in the Duplicate/Duress Passcodes field because both of these passcodes share "478" as the first three digits. If Passcode Length were changed from four digits to three digits, all of these passcodes would become duplicate passcodes of "478."

Reference

Miscellaneous > Passcode Length

Swinger Bypass Count

Default: 2

Selections: 1 to 4

When a point has Swinger Bypass set to **Yes**, the value set in this parameter determines the number of times the point is erroneously faulted within an hour before it is automatically bypassed.

IMPORTANT:

- To comply with SIA CP-01 False Alarm Reduction, set this parameter to either **1** or **2**. See SIA CP-01 Verification for more information.
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **4**.

Option	Description
1 or 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.

Reference
Miscellaneous > Swinger Bypass Count

Remote Warning

Default: No
Selections: Yes or No
This parameter pulses the alarm bell once (2-sec **ON**, then OFF) when the assigned area is remotely armed, and twice (2-sec **ON**, 2-sec OFF, 2-sec **ON**, then OFF) when the area is remotely disarmed. This parameter also applies to keyswitch arming and disarming.

IMPORTANT:
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. See SIA CP-01 Verification for more information.
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **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 (keyswitch or keyfob).
No: No remote warning occurs to annunciate the arming or disarming of an area through remote software, or a remote arming device (keyswitch or keyfob).
Reference
Miscellaneous > Remote Warning

Crystal Time Adjust

Default: No
Selections: Yes or No
This parameter determines how the control panel regulates its clock time.
Yes: The control panel uses the on-board crystal frequency to regulate its clock time.
No: The control panel uses traditional AC frequency to regulate its clock time.
IMPORTANT: When upgrading from a G-series control panel account that does not support this feature to a GV4 control panel account, RPS forces the default to **No**.
Reference
Miscellaneous > Crystal Time Adjust

Part On Output

Default: No
Selections: Yes or No
When set to **Yes**, the Fail to Close outputs become the Part On outputs. This output is activated when all areas assigned to the same output are armed Part On Instant or Part On Delayed.

When set to **No**, the Fail to Close outputs operate when the closing window expires for the specified area.

IMPORTANT: When upgrading from a G-series control panel account that does not support this feature to a GV4 control panel account, RPS forces the default to **No**.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Part On Output

Early Area Armed Output

Default: No

Selections: Yes or No

When set to **Yes**, the Area Armed or the Part On output activates at the start of Exit Delay time.

When set to **No**, the area wide armed output types continue to activate at the end of Exit Delay time.

IMPORTANT: When upgrading from a G-series control panel account that does not support this feature to a GV4 control panel account, RPS forces the default to **No**.

RPS Menu Location

Miscellaneous > Early Area Armed Output

Daylight Saving Time

Default: US Calendar

Selections:

- Disabled
- US Calendar

To enable this parameter, select **US Calendar**. The control panel will adjust its clock according to US daylight saving rules.

To disable this parameter, select **Disabled**. The control panel will not adjust its clock.

Reference

Miscellaneous > Daylight Saving Time

Time Zone

Default: [UTC-05:00] Eastern Time (US & Canada)
Selections: Time Zones and UTC

Time Zone
(UTC-12:00) International Date Line West
(UTC-11:00) Midway Island, Samoa
(UTC-10:00) Hawaii
(UTC-09:00) Alaska
(UTC-08:00) Pacific Time (US & Canada)
(UTC-08:00) Tijuana, Baja California
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
(UTC-06:00) Central America
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Guadalajara, Mexico City, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogota, Lima, Quito
(UTC-05:00) Eastern Time (US & Canada)
(UTC-05:00) Indiana (East)
(UTC-04:30) Caracas
(UTC-04:00) Asuncion
(UTC-04:00) Atlantic Time (Canada)
(UTC-04:00) Georgetown, La Paz, San Juan
(UTC-04:00) Manaus
(UTC-04:00) Santiago
(UTC-03:30) Newfoundland
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires
(UTC-03:00) Cayenne
(UTC-03:00) Greenland
(UTC-03:00) Montevideo
(UTC-02:00) Mid-Atlantic
(UTC-01:00) Azores
(UTC-01:00) Cape Verde Is.
(UTC) Casablanca
(UTC) Coordinated Universal Time
(UTC) Dublin, Edinburgh, Lisbon, London
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(UTC+01:00) West Central Africa
(UTC+02:00) Amman
(UTC+02:00) Athens, Bucharest, Istanbul
(UTC+02:00) Beirut
(UTC+02:00) Cairo
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC+02:00) Jerusalem
(UTC+02:00) Minsk
(UTC+02:00) Windhoek
(UTC+03:00) Baghdad
(UTC+03:00) Kuwait, Riyadh
(UTC+03:00) Moscow, St. Petersburg, Volgograd
(UTC+03:00) Nairobi
(UTC+03:00) Tbilisi
(UTC+03:30) Tehran
(UTC+04:00) Abu Dhabi, Muscat
(UTC+04:00) Baku
(UTC+04:00) Port Louis
(UTC+04:00) Yerevan
(UTC+04:30) Kabul
(UTC+05:00) Ekaterinburg
(UTC+05:00) Islamabad, Karachi
(UTC+05:00) Tashkent
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayawardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Almaty, Novosibirsk
(UTC+06:00) Astana, Dhaka
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoi, Jakarta
(UTC+07:00) Krasnoyarsk
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
(UTC+08:00) Irkutsk, Ulaan Bataar
(UTC+08:00) Kuala Lumpur, Singapore
(UTC+08:00) Perth
(UTC+08:00) Taipei

(UTC+09:00) Osaka, Sapporo, Tokyo
(UTC+09:00) Seoul
(UTC+09:00) Yakutsk
(UTC+09:30) Adelaide
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Vladivostok
(UTC+11:00) Magadan, Solomon Is., New Caledonia
(UTC+12:00) Auckland, Wellington
(UTC+12:00) Fiji, Marshall Is.
(UTC+12:00) Petropavlovsk-Kamchatsky
(UTC+13:00) Nuku'alofa

This parameter identifies the time zone for the region where the control panel is installed.

Reference

Miscellaneous > Time Zone

4 Area Wide Parameters

4.1 Area/Bell Parameters, Open/Close Options

Area On

Default:
- Area 1: Yes
- All other areas: No

Selections: Yes/No

IMPORTANT:
- Area 1 must be enabled. System events such as power and phone supervision do not report correctly if Area 1 is disabled.
- The D9412GV4 supports up to 32 areas, theD7412GV4 supports up to 8 areas.
- To meet UL864 requirements, set this parameter to **Yes**.

Use this parameter to enable or disable the specified area.

When an area is set to No, the following conditions occur:
- Points assigned to this area do not generate events.
- When arming and disarming, this area number is not displayed at keypads with the scope to view this area.
- Status for this area is not reported with status reports.
- All user authority in this area is turned off while the area is disabled.

Yes: Area is enabled.

No: Area is disabled.

Reference

Area Wide Parameters > Area/Bell Parameters > Area On

Account Number

Default: 0000

Selections: 4 to 10 digits, 0-9, B-F

This parameter determines the account number reported 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 may share the same account number. The control panel uses the account number as a reference for arming and keypad text displays. Enter a maximum of 10 characters (0-9, B-F).

CAUTION:
- Make sure your automation software is compatible with 10-digit account numbers before programming a 10-digit account number in a GV4 Series control panel.
- Account numbers must not include "A" for any digit.

Reference

Area Wide Parameters > Area/Bell Parameters > Account Number

Force Arm/Bypass Max

Default: 2

Selections:
- **D9412GV4:** 0-99
- **D7412GV4:** 0-30

Specify the maximum number of combined controlled points that can be faulted or in a bypassed state when arming this area.
See FA Returnable and BA Returnable in the Point Index for returning a point to the system when the point returns to normal or when the area is disarmed.

IMPORTANT:
- Points must have Bypassable set to Yes to be bypassed or force armed. Force arming does not bypass 24-hour points.
- To comply with UL1610, set this parameter to **0** for wireless keyfobs.

Reference
Area Wide Parameters > Area/Bell Parameters > Force Arm/Bypass Max

Delay Restorals

Default: No
Selections: Yes/No
Use this parameter to delay restoral reports until bell time expires.
Yes: Point restoral reports are not to be sent until the bell time expires or user acknowledges alarm condition.
No: Restoral reports are sent when point restores, regardless of bell time.
Reference
Area Wide Parameters > Area/Bell Parameters > Delay Restorals

Exit Tone

Default: Yes
Selections: Yes/No
This parameter sounds an exit tone during exit delay at all keypads assigned to this area.

IMPORTANT: Exit tones for individual keypads (based on their KP# 1 through 16) can be turned off by setting KP# Exit Tone to No.

Reference
Area Wide Parameters > Area/Bell Parameters > Exit Tone

Exit Delay Time

Default: 300
Selections: 0 to 600 (in 5 second increments)
Set the exit delay time for this area when All On Exit or Part On Exit arming is used.

IMPORTANT:
- Points programmed for instant alarms generate alarms immediately, even during exit delay. To prevent instant alarms on interior points when leaving the building, then configure those points with a Point Index with P## Type of Interior Follower.
- To comply with SIA CP-01 False Alarm Reduction, set this parameter between 45 and 255 seconds. See SIA CP-01 Verification for more information.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters > Exit Delay Time

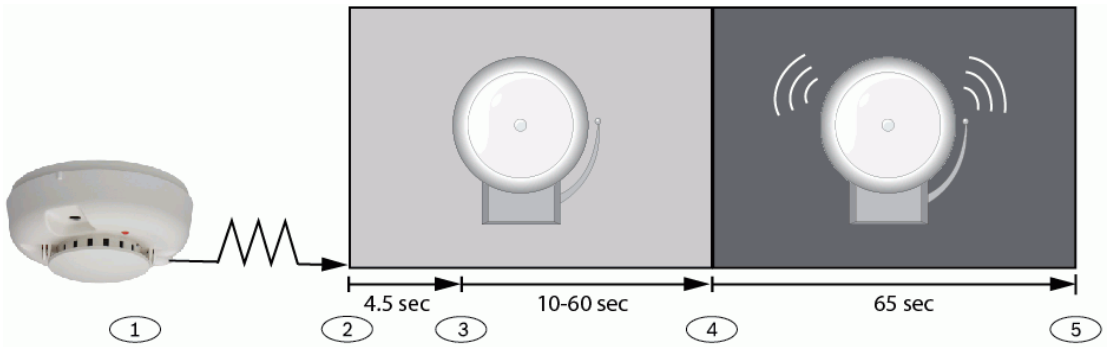
Auto Watch

Default: No
Selections: Yes/No
Set this parameter to automatically put the area in Watch Mode when the control panel is disarmed.
IMPORTANT: Controlled points programmed as P## Watch Point , automatically send a watch tone. When the control panel is Part On, only interior points activate the watch tone when Watch Mode is turned on. Part On points still report as alarms or troubles.
Yes: When the area is disarmed, Watch Mode is turned on automatically.
No: When the area is disarmed, Watch Mode must be turned on or off manually.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters > Auto Watch

Verify Time

Default: 5
Selections: 5 to 55 seconds (in 1 second increments)
This parameter sets the length of time to wait for the sensor to stabilize after an alarm verification point is faulted and the sensor reset has reapplied power to the sensors. This allows the control panel to re-check alarm verification point activations before generating alarm signals.
Alarm verification is a feature of fire detection and alarm systems to reduce false alarms where sensors report alarm conditions for a minimum period of time, or confirm alarm conditions within a given period of time after being reset, in order to be accepted as a valid alarm initiation signal.
IMPORTANT:
- Do not enable the Cross Point Feature in Point Indexes that are designated for fire points.
- Check the sensor's datasheet for the stabilization time and enter a value at least 5 seconds higher than the longest time specified by any sensor in the loop.
- Check with your Authority Having Jurisdiction (AHJ) to determine the maximum verification time allowed.

Alarm verification points are programmed individually to activate the verification feature. Refer to *Point Index*. Any resettable fire point can activate alarm verification for the area to which it is assigned. Bosch recommends using separate area alarm verification outputs.
To enable alarm verification on a point, set Point Type to **Fire**, and Alarm Verify and Resettable to **Yes**.
When an alarm verification point is faulted, the control panel automatically removes power from all resettable points connected to the areas Reset Sensors output. Power is removed for 4.5 seconds. Whenever a sensor reset is performed (manually from the keypad or automatically as part of the alarm verification process), the control panel ignores alarm or trouble conditions from the resettable points for the amount of time programmed in Restart Time. After Restart Time has expired, a 65 second confirmation window begins. If the alarm verification point is still in alarm, or faults again during the confirmation window, or if a different alarm verification point in the area faults, an alarm is generated.



Callout - Description
1 - Sensor detects possible event.
2 - Power removed from resettable points.
3 - Power reapplied to resettable points. Verify Time begins.
4 - Confirmation window begins. Any alarm during this period will be annunciated.
5 - Confirmation window ends. The sequence is re-initiated the next time an alarm verification point is faulted.

Reference
Area Wide Parameters > Area/Bell Parameters > Restart Time

Duress Enable

Default: No
Selections: Yes/No
This parameter determines if this area allows duress alarms to be generated. See Duress Type an explanation of Duress.

IMPORTANT:
- To comply with SIA CP-01, set this parameter to **Yes**.
- If you set the parameter to **No** in a particular area, the passcode you normally enter for Duress is no longer valid in that area.
- If this parameter is set to **No**, and a passcode with the appropriate disarm authority is used to duress-disarm the area, `NO AUTHORITY` appears in the keypad display.
- If Go To Area [MENU][3][5] is used to move the keypad display to an area where this parameter is set to **No**, a valid duress disarm passcode **does not** send a duress report.

Yes: Enable Duress alarm for this area.
No: Disable Duress alarm for this area.
Reference
Area Wide Parameters > Area/Bell Parameters > Duress Enable

Area Type

Default: Regular
Selections:
- Regular
- Master
- Associate
- Shared

This parameter is used to define boundaries between areas. Boundaries are defined in terms of whether an area can be armed while a user is in another area, whether an area automatically arms when another area is armed, or whether an area requires other areas be armed before it is armed.

Regular Will arm or disarm as an independent area.

Master Will not allow arming for this area unless all Associate areas with the same A# Acct Number are all on exit delay arming or All On. *Check Area* displays if the Associate areas have not yet been 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.

IMPORTANT:
Keypad Scope affects master arming. When arming a master area from a keypad with Keypad Scope set to Panel Wide or Account Wide, all Associate areas enter 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.

IMPORTANT:
Using the arming sked 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 occurs before all Associate areas are armed.

Associate Will allow arming and disarming regardless of the armed state of the other areas with the same A# Acct Number . This type of area is used with a Master Area and is associated by having the same account number. To schedule the arming of a Master area, two Sked Functions must be configured to execute in sequence. The first sked must arm all Associate areas, then the second must arm the Master area(s). Keypads assigned to Associate areas, when used in conjunction with Shared areas, should have the KP# Scope programmed to encompass the Shared Area.

IMPORTANT:
Keypads assigned to Associate areas, when used with Shared areas, must have Keypad Scope programmed.

Shared **Shared** areas cannot be armed using a passcode, keyswitch, sub-control, Sked, Custom Functions, automation, or by RPS.

Shared Area Characteristic	Description
Arming a Shared Area	Requires all Associate areas to be armed. As soon as the last Associate area is armed, the Shared area begins its arming sequence automatically. Shared

	areas can not be armed by passcode, keyswitch, sub-controls or RPS. To allow faulted points to be displayed at associated areas, the shared and associate areas must share the same account number.
Disarming a Shared Area	Shared areas automatically disarm when any Associate area in the panel is disarmed. Shared areas can not be disarmed by passcode, tokens/cards, keyswitch, sub-controls or RPS.
Shared Area Arming Sequence	When Shared areas automatically begin to arm, the arming is based on the A# Exit Dly Time programmed for the ***Area #*** where the keypad has been assigned.
Shared Area Not Ready	If a point is faulted in the Shared area, *Check Area* will display on the Associate keypad that is arming the last Associate area. Associate area Keypads can display faults from Shared areas as long as the Shared areas fall within the scope of the Associate area.
Force Arming a Shared Area	When *Check Area* is displayed, press the NEXT key until the Force Arm? prompt is shown. Pressing the ENTER key will force arm 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 max amount for the Shared area. Remember to include the Shared area in the Associate area's scope.
Viewing Shared Area Armed Status	[VIEW AREA STATUS] can be used from a keypad outside of the Shared area to view the Shared areas armed state.
Silencing Sounders in the Shared Area	Shared area alarms and troubles can be silenced from any keypad. To silence sounders, the user must have an authority level assigned to the Shared area.
Access Control Readers Assigned to the Shared Area	If the entry area is armed and is a Shared area, then the exit delay will restart and allow a user to walk to an Associate area and disarm. If the token/card reader assigned to the Shared area includes *any* Associate area in the D## KP# Scope (in the ACCESS CONTROL section, both the Associate area and Shared area will disarm when the token/card is presented.
Closing Reports for Shared Areas	If closing reports for Shared areas are required, Passcodes must also have a valid authority level assigned in the Shared area.

The scope of all Associate areas must include the Shared area(s) in order to view faulted points.

IMPORTANT:
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.

The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8areas.

Reference

Area Wide Parameters > Area/Bell Parameters > Area Type

Two Man Rule?

Default: No

Selections: Yes/No

Set this parameter to Yes to require that two valid passcodes are entered, *using the same keypad*, to disarm the area. It is recommended that you use this parameter in an area that is disarmed from All On using a keypad with Area Wide scope. An alarm condition occurs if entry delay ends before the second valid passcode is entered.

If the area is already in an alarm condition, the first passcode entry silences the alarm. The second passcode entry disarms the area.

If the second passcode is entered using a different keypad than the first passcode, the second keypad displays a warning that the Two Man Rule is already running. Enter both passcodes using the same keypad.

The area scope that is disarmed is determined by the first passcode that starts the Two Man Rule. A single area keypad (with Area Wide scope) is required for this feature.

You can create a custom function that will disarm the area using passcode disarm.

Set this parameter to Yes in facilities that require a higher level of security to gain access to the secured area. For example, a bank might enable this parameter to gain access to the vault.

IMPORTANT:

- If this parameter is enabled, set the Scope parameter for keypads in the affected areas to "Area Wide."
- You should not set Two Man Rule to Yes in an area that also has Early Ambush set to Yes.
- This function only works when you use passcode disarm.
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to **No** for all enabled areas. See SIA CP-01 Verification for more information.

Yes: Two valid and unique passcodes, entered using the same keypad, are required to disarm the area.

No: One passcode with a valid authority level can disarm the area.

Reference

Area Wide Parameters > Area/Bell Parameters > Two Man Rule

Early Ambush?

Default: No

Selections: Yes/No

Set this parameter to Yes to require two valid passcodes to disarm the area within the time limit set in the Early Ambush Time parameter. The first passcode entry disarms the area, and the second passcode entry validates the disarm command. The passcodes can be entered from any two keypads in the area.

It is recommended that you use this parameter when disarming from a master area, or during the entry delay period for All On.
You can create a custom function that will disarm the area using passcode disarm.

IMPORTANT:
- If the second passcode is not entered before the Early Ambush Time ends, the control panel generates a duress event based on the primary user.
- You should not set Early Ambush to Yes in an area that also has Two Man Rule set to Yes.
- This function only works when you use passcode disarm.
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to **No** for all enabled areas. See SIA CP-01 Verification for more information.

Yes: Two valid passcodes are required to disarm the area within the time limit set in the Early Ambush Time.
No: One passcode with a valid authority level can disarm the area.
Reference
Area Wide Parameters > Area/Bell Parameters > Early Ambush

Fire Time

Default: 6
Selections: 1 to 90 minutes (in one minute increments)
Enter the number of minutes the bell rings for fire alarm points. The output activated for this time is programmed in A# Fire Bell. The A## Gas Bell is completely independent of the A## Fire Bell, but also follows the time programmed in this prompt.
The bell output starts as soon as the fire alarm occurs. It shuts off the bell when the programmed number of minutes expires.
If programmed for 1 minute, the output might last anywhere from 0 to 60 seconds of bell time. Set this parameter for two minutes or more to ensure you have ample output time.

IMPORTANT:
- Check with your Authority Having Jurisdiction (AHJ) to determine the appropriate bell time for your geographical area.
- To meet UL864 requirements, set this parameter to at least 5 minutes. Verify with the Authority Having Jurisdiction for local requirements.

Reference
Area Wide Parameters > Area/Bell Parameters > Fire Time

Fire Pattern

Default: Pulsed
Selections:
- Steady
- Pulsed
- California Standard
- Temporal Code 3

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

IMPORTANT: When two fire points sharing the same output go into alarm, the bell pattern of the most recent fire event takes precedence.

Steady: Steady output.
Pulsed: Pulsed march time. 60 beats per minute at an even tempo (0.5 seconds on and 0.5 seconds off).

California Standard (CA): 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent. This sequence repeats until bell time expires.
Temporal Code 3 (TempCode3): 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off; pattern repeats. This sequence repeats for a minimum of 3 minutes with ± 10% timing tolerance. (1999 NFPA standards allow automatic silencing as permitted by the Authority Having Jurisdiction (AHJ), and carry a minimum ring time of 5 minutes.)
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fire Pattern

Burg Time

Default: 6
Selections: 1 to 90 minutes (in one minute increments)
Enter the number of minutes the bell rings for burglary alarm points. The output activated for this time is programmed in A# Alarm Bell.
The bell output starts 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. Set this parameter for two or more minutes.

IMPORTANT:
- Check with your Authority Having Jurisdiction (AHJ) to determine the appropriate bell time for your geographical area.
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to 6 minutes or higher in all enabled areas. See SIA CP-01 Verification for more information.

Reference
Area Wide Parameters > Area/Bell Parameters > Burg Time

Burg Pattern

Default: Steady
Selections:
- Steady
- Pulsed
- California Standard
- Temporal Code 3

Select the bell pattern this area uses to signal an alarm on a non-fire point.
Steady: Steady output.
Pulsed: Pulsed march time. 60 beats per minute at an even tempo (0.5 seconds on and 0.5 seconds off).
California Standard (CA): 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent. This sequence repeats until bell time expires.
Temporal Code 3 (TempCode3): 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off; pattern repeats. This sequence repeats for a minimum of 3 minutes with ± 10% timing tolerance. (1999 NFPA standards allow automatic silencing as permitted by the Authority Having Jurisdiction (AHJ), and carry a minimum ring time of 5 minutes.)
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Burg Pattern

Gas Pattern

Default: Temporal Code 4
Selections:
- Steady
- Pulsed
- California Standard
- Temporal Code 3
- Temporal Code 4

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

IMPORTANT: When two fire points sharing the same output go into alarm, the bell pattern of the most recent fire event takes precedence.

Steady: Steady output.
Pulsed: Pulsed march time. 60 beats per minute at an even tempo (0.5 seconds on and 0.5 seconds off).
California Standard (CA): 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent. This sequence repeats until bell time expires.
Temporal Code 3 (TempCode3): 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off; pattern repeats. This sequence repeats for a minimum of 3 minutes with ± 10% timing tolerance. (1999 NFPA standards allow automatic silencing as permitted by the Authority Having Jurisdiction (AHJ), and carry a minimum ring time of 5 minutes.)
Temporal Code 4 (TempCode4): 0.1 seconds On, 0.1 seconds Off, 0.1 seconds On, 0.1 seconds Off, 0.1 seconds On, 0.1 seconds Off, 0.1 seconds On, 5 seconds Off; pattern repeats. (On Zonex outputs, this pattern is modified to four pulses of 0.5 seconds on/off with a 5 second pause and is not NFPA compliant).
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Gas Pattern

Single Ring

Default: No
Selections: Yes/No
This parameter determines if an alarm from a non-fire point can restart the alarm bell time with each alarm event, or only initiate alarm output once per arming period. This parameter does not silence the keypad alarm bell tone, nor prevent any reports. This parameter does not affect fire points. Fire points restart bell time with each new alarm.

IMPORTANT:
- If an alarm occurs on a 24-hour point while the area is disarmed, arming that area with a keyswitch does not clear the Single Ring flag.
- Silencing the bell resets Single Ring.

Yes: One bell output per arming period. After one alarm, alarms on non-fire points in the same area can not restart the bell until the armed state changes.
No: Restart bell output with each alarm event.
Reference
Area Wide Parameters > Area/Bell Parameters > Single Ring

Bell Test

Default: No
Selections: Yes/No
Provide alarm output from the output programmed at A# Alarm Bell after the closing report has been confirmed or the exit delay time has expired.

Bell Test After Closing Confirmation
In areas that report opening and closing activity, the bell test occurs after the control panel sends the closing report and receives the acknowledgment from the central station receiver. For proper operation of the bell test after closing confirmation, the following rules apply:

- The control panel must report opening and closings to the central station.
- Restricted openings and closings, and opening and closing windows, should not be used.

Area Armed Confirmation
In areas that do not report opening and closing activity, the alarm bell output for this area is activated for two seconds after exit time expires.

IMPORTANT: When more than one area is armed at the same time (for example, ARM ALL AREAS? function is used), the bell sounds for two seconds with a two-second pause between each bell activation if all areas have the same exit delay time programmed. Otherwise, the bell test occurs as each area is armed and it complete its exit delay time. When areas are armed simultaneously and report to the central station, the bell test occurs as each area is confirmed by the central station receiver.

Yes: Initiate bell test.
No: Do not initiate bell test.
Reference
Area Wide Parameters > Area/Bell Parameters > Bell Test

Account O/C

Default: No
Selections: Yes/No
This parameter determines if account opening and closing reports are generated by this area. Set this parameter the same for all areas in the account.

IMPORTANT: Account numbers are sent over the network to the central station receiver.

Yes: Send opening and closing reports by account.
Use this selection if the control panel sends reports to an automation system that cannot interpret multiple area opening/closing reports.
An account opening report is generated when the first area in an account is opened (disarmed). After the account opening report is sent, disarming other areas in the account does not generate another account opening report. An account closing report is generated only when the last area in an account is closed (armed). Account opening and closing reports do not contain any area information.

IMPORTANT: 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 set to Yes, the report is not sent. Bosch recommends that all areas sharing the same account number use the same opening and closing window times.

No: Do not send opening and closing reports by account.
Reference
Area Wide Parameters > Area/Bell Parameters > Account O/C

Area O/C

Default: Yes
Selections: Yes/No
This parameter determines if the area number and the account number are sent upon arming and disarming. As long as A# Acct O/C is set to No, the account number is sent when arming this area individually. If A# Acct O/C is set to Yes, all areas with the same account number must also be armed.
An area opening report is generated when each individual area is opened (disarmed).
An area closing report is generated when each individual area is closed (armed).
IMPORTANT: Do not set this parameter to Yes if the control panel sends reports to an automation system that cannot interpret multiple area opening/closing reports.
Opening/Closing Reports are only sent for users with Authority Levels assigned as follows
- **Ready to Arm:** Area Open/Close = E
- **Not Ready to Arm (Force Arm/Bypass Arm):** Restricted Open/Close = E
- **Part On:** Part On Open/Close = E

Yes: Include the area number and generate opening and closing reports for this area when it is armed.
No: Do not include the area number or generate opening and closing reports for this area.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters > Area O/C

Disable O/C in Window

Default: Yes
Selections: Yes/No
This parameter 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.
Yes: Do not send opening and closing reports to the central station if they occur inside an active window.
If an opening or closing report occurs outside of a window, send it with an early or late modifier. See O/C Windows.
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.
If you want to monitor all opening and closing activity, but you also want to use features provided by opening and closing windows, set this parameter to No, and program appropriate O/C windows.
Reference
Area Wide Parameters > Area/Bell Parameters > Disable O/C in Window

Auto Close

Default: No
Selections: Yes/No
With this parameter, the control panel can automatically all on-arm the area at the end of the closing window regardless of the previous armed state.
IMPORTANT: Regardless of A# Force Arm Max or P## Bypassable , an unconditional force arm occurs resulting in faulted points left out of the system until they return to normal.
Yes: The area automatically all on-arms at the end of the close window.
When the area automatically arms, the control panel sends a closing report if area and/or account reports are programmed to do so.
No: Do not automatically arm the area at the end of the close window.
Reference
Area Wide Parameters > Area/Bell Parameters > Auto Close

Fail To Open

Default: No
Selections: Yes/No
This parameter allows you to determine if a FAIL TO OPEN report is sent for this area. This parameter can also be used to determine if a user failed to disarm the area before the opening window expired. Normal opening and closing reports do not need to be programmed to use this parameter.
Yes: A FAIL TO OPEN report is sent for this area if the area is not disarmed when the opening window stop time occurs.
No: A FAIL TO OPEN report is not sent for this area.
Reference
Area Wide Parameters > Area/Bell Parameters > Fail to Open

Fail To Close

Default: No
Selections: Yes/No
This parameter allows you to determine if a FAIL TO CLOSE report is sent for this area. This parameter can also be used to determine if a user failed to arm the area before the closing window expired. Normal opening and closing reports do not need to be programmed to use this parameter.
If A# Auto Close is set to Yes, a FAIL TO CLOSE report is sent because it occurs when the closing window stop time occurs.
If A# Disable O/C in Window is set to Yes, the FAIL TO CLOSE report is followed by CLOSING LATE or F(orce) CLOSE LATE report.
IMPORTANT: An exit delay time must be programmed in A# Exit Dly Time.
Yes: A FAIL TO CLOSE report is sent for this area if the area is not armed when the closing window stop time occurs.
No: A FAIL TO CLOSE report is not sent for this area.
Reference
Area Wide Parameters > Area/Bell Parameters > Fail to Close

Latest Close Time

Default: Disabled
Selections:
- Disabled
- 00:30 to 23:30 (half-hour increments)
- Midnight

Use this parameter to set a latest close time boundary when an open/close window is assigned to the selected area.
If you select **Disabled**, RPS sends 0:00 to the control panel.
If you select **Midnight**, RPS sends 24:00 to the control panel.

IMPORTANT: If the Lastest Close Time setting is set to a non-zero value, the time of day specified in the Close Window Start parameter cannot be greater than or equal to the Latest Close Time setting. For example, if the Latest Close Time parameter is set to 17:30, the Close Window Start parameter cannot be set to 17:30 or higher.

Reference
Area Wide Parameters > Area/Bell Parameters > Latest Close Time

Restricted O/C

Default: No
Selections: Yes/No
This parameter determines if this area can restrict opening and closing report activity. A restricted opening report means the control panel sent an area opening report only when the area is disarmed after a non-fire alarm.
A restricted closing report means the control panel sent an area closing report only when the area has been All On with controlled points that were faulted during the arming sequence. The sequence of reports generated by a restricted closing are: WAS FORCE ARMED, FORCED POINT, FORCED CLOSE.
Windows do not prevent restricted opening and closing reports from being sent. Early or late designations are not added to opening/closing reports when they are sent according to the rules for restricted opening/closing reports.
Yes: Restrict opening and closing reports for this area. A# Area O/C must be set to Yes to generate restricted opening and closing reports.

IMPORTANT: If a passcode is not required for arming or disarming and this parameter is set to Yes, the area only sends restricted opening and closing reports. In this case, restricted reports are sent without user ID.

No: Do not restrict opening and closing reports for this area. Regardless of programming in L## Restricted O/C , reports are not restricted in this area when this item is set to No.

IMPORTANT: WAS FORCE ARMED and FORCED CLOSE events are still sent to the central station if enabled in routing when force arming the system.

Reference
Area Wide Parameters > Area/Bell Parameters > Restricted O/C

Part On O/C

Default: No
Selections: Yes/No
This parameter determines if this area can send Part On instant and Part On delay closing reports and normal opening reports to the central station. This event is not suppressed by opening/closing windows.
Yes This area can send Part On opening and closing reports.

No This area cannot send Part On opening and closing reports.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters > Part On O/C

Exit Delay Restart

Default: Yes
Selections: Yes or No
When this parameter is set to **Yes**, it activates when a controlled point with delay alarm response changes from normal to faulted and back to normal during Exit Delay. When activated, if any controlled point in the same area with delay alarm response is faulted, Exit Delay restarts. Exit Delay continues until it expires or the area changes arming states. This operation can occur only once in an arming cycle.
IMPORTANT: When upgrading from a G-series control panel account that does not support this feature to a GV2/GV4 control panel account, RPS forces the default to **No**.
Yes: Delay armed points in this area restart Exit Delay one time.
No: Delay armed points continue to count down normally if faulted during Exit Delay.
Reference
Area Wide Parameters > Area/Bell Parameters > Exit Delay Restart

All On - No Exit

Default: Yes
Selections: Yes or No
Select whether or not the arming state for an area changes from All On to Part On if no Part On points with delay response are faulted during Exit Delay. This feature does not operate in areas with Area Type set to Shared.
Only the final armed state is reported and displayed at the keypads.
IMPORTANT: When upgrading from a G Series control panel account that does not support this feature to a GV2/GV4 control panel account, RPS forces the default to **No**.

Yes	Switch the arming state of the area from All On Delay to Part On Delay if no Part On Delay points are faulted and restored during the exit delay time.
No	Keep the arming state of the area All On Delay if no Part On Delay points are faulted and restored during the exit delay time.

When arming from a keyfob, the panel ignores this option. The area is always All On per ANSI/SIA CP-01 as the keyfob is a remote control device.
Reference
Area Wide Parameters > Area/Bell Parameters > All On - No Exit

Exit Delay Warning

Default: No
Selections: Yes or No
When this parameter is set to **Yes**, the alarm bell pulses on and off every two seconds for the remaining 10 sec of Exit Delay.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. See SIA CP-01 Verification for more information.
Yes: Pulse the alarm output for the last 10 sec of Exit Delay
No: Do not pulse the alarm output during Exit Delay
Reference
Area Wide Parameters > Area/Bell Parameters > Exit Delay Warning

Entry Delay Warning

Default: No
Selections: Yes or No
When this parameter is set to **Yes**, the alarm bell pulses on and off every two seconds for the remaining 10 sec of Entry Delay.

IMPORTANT:
- To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. See SIA CP-01 Verification for more information.
- When upgrading from a G-series control panel account that does not support this feature to a GV4 control panel account, RPS forces the default to **No**.

Yes: Pulse the alarm output for the last 10 sec of Entry Delay
No: Do not pulse the alarm output during Entry Delay
Reference
Area Wide Parameters > Area/Bell Parameters > Entry Delay Warning

Area Re-Arm Time

Default: 00:00
Selections: 00:00 thru 23:59
00:00 = disabled
This parameter sets the length of time (HH:MM) that a disarmed area will delay until it rearms to All On Delay. Use Extend Close to lengthen an active rearm delay. Although this is a relative timer, the area will automatically rearm at midnight regardless of when the timer started. Upon rearming, any points not ready to arm are force armed. For example, if the Area Re-Arm timer is configured to be 4 hours and the area is disarmed at 10:30pm, then the timer will be automatically truncated to terminate at 11:59pm.

IMPORTANT
Force Arm / Bypass Max is ignored when rearming.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Re-Arm Time

Area Name Text

Default: AREA # Name Text (# = the Area number)
Selections: Up to 32 alphanumeric characters.
This parameter sets what is displayed at keypads. This is for informational purposes only.
Enter up to 32 characters of text to describe the area.
- SDI2 keypads display the first 20 characters. If more than 20 characters are used, the text scrolls across the display one time. To scroll the text again, press [ESC].
- Spaces before, after and within a string of text are treated as text and are included in the 32 character limit.
- On SDI keypads, only the first 16 characters display.

The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.
RPS Menu Location
Area Wide Parameters > Area Name Text

5 Keypads

5.1 SDI2 Keypad Assignments

Keypad Type

Default:
- Address 1 = B92x Two-line keypad
- Address 2-16 = No Keypad Installed

Selections:
- No keypad installed
- B91x Basic keypad
- B92x Two-line keypad
- B93x ATM style keypad
- B94x Touch screen keypad

This parameter identifies the type of keypad that is connected to the control panel at this address. The information in this parameter is auto-configured when the keypad is first installed. The B93x ATM style keypad has a 5-line display and soft keys.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Keypad Type

Area Assignment

Default: 1

Selections:
- D9412GV4: 1 to 32
- D7412GV4: 1 to 8

This parameter identifies the area number in which you are installing this keypad or keypads with this address and the same rotary switch settings.

The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

The D9412GV4 supports up to 32 areas, and the D7412GV4 supports up to 8 areas.

Reference

Keypads > SDI2 Keypad Assignments > Area Assignment

Scope

Default:
- Address 1: Panel Wide
- Addresses 2-16: Area Wide

Selections:
- Area Wide
- Account Wide
- Panel Wide
- Custom

Use this parameter to define what areas are affected when this keypad is armed, what areas can be viewed with this keypad, and what areas this keypad can move to.

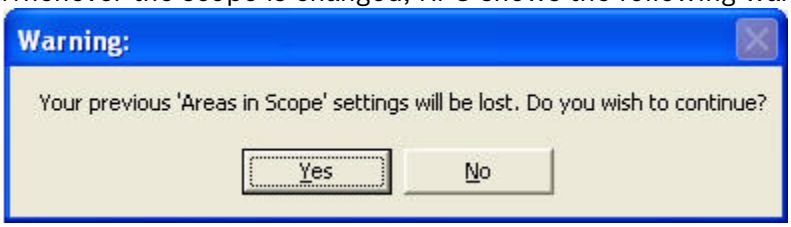
Area Wide: An area keypad is restricted to the viewing information and arming/disarming functions for the area to which it is assigned.

Account Wide: An account keypad can view information, and perform arming and disarming functions for all areas that have the same Acct Number. This is normally used for an associate area.

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.

Custom: A custom keypad has no keypad restrictions.

Whenever the scope is changed, RPS shows the following warning dialog:



– If you click **Yes**, RPS resets the Area(s) In Scope parameter.
– If you click **No**, no changes are made in RPS.

The D9412GV4 and D7412GV4 support up to 16 keypads.
The Areas in Scope parameter in the D7412GV4 is automatically set according to the option selected in this parameter.

Reference
Keypads > SDI2 Keypad Assignments > Scope

Area(s) In Scope

Default:
– KP Address 1: All (Areas 1-8)
– All other KP Addresses: none

Selections:
– D9412GV4: 1 to 32
– D7412GV4: 1 to 8

IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.

This parameter 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.

Reference
Keypads > SDI2 Keypad Assignments > Areas in Scope

Passcode Follows Scope

Default: Yes
Selections: Yes/No

Yes User can change the armed state of all areas within the scope of this keypad.

No User can only change the armed state of the area assigned to the keypad.

Use this parameter to create a group of account wide keypads that arm only the area to which they are assigned, even if the user has a passcode with arming or disarming authority rights in all areas.
Cards and tokens disarm according to this parameter. If this parameter is set to No, cards and tokens disarm only the area to which the door's associated keypad is assigned.
Users must have authority enabled in Passcode Arm and Passcode Disarm. This parameter does not affect the Function List arming and disarming parameters.
The user must have disarming rights for cards and tokens programmed at the disarm level, but does not need disarming and arming authority for the keypad.
If the area to which this keypad is assigned is armed, entering a valid passcode disarms this area and all other areas assigned to the scope of this keypad.
If the area to which this keypad is assigned is disarmed, entering a valid passcode disarms this area and all other areas assigned to the scope of this keypad.
The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Reference
Keypads > SDI2 Keypad Assignments > Passcode Follows Scope

Enter Key Output

Default: 0 (for all KP addresses)
Selections:
- **D9412GV4:** 0 to 128, A, B, C
- **D7412GV4** 0 to 64, A, B, C

This parameter provides a low-level access control strike on a door. This parameter does not shunt a point.
IMPORTANT: Passcode Enter Function cannot be set to "Cycle Output" unless this parameter is set to a value other than “0”.
0 (zero): The [ENTER] key is not used to cycle a output.
1 to 128, A, B, C: Assign the output number that activates when Passcode Enter function is used at this keypad.
A, B, C: Assigned onboard output that cycles when Passcode Enter function is used.
Enter the output number that momentarily activates for 10 seconds when a user enters a valid passcode and presses [ENTER] on the keypad. Two events might be generated when this function is used: Output ### Set with User ID and, Output ### Reset without User ID.
Entering a valid code and pressing [ENTER] silences the bell tone.
When programmed to activate a output, the keypad's passcode function cannot be used for any other function. Outputs used for this function must not be shared with any other point, sensor reset, control panel or bell functions. Doing so can cause erroneous output operation.
The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Reference
Keypads > SDI2 Keypad Assignments > Enter Key Output

Passcode Enter Function

Default: Arm/Disarm (all KP addresses)
Selections:

Arm/Disarm	Passcode + [ENTER] key will start All On Delay Arm for all areas within the users authorized scope if the current area is disarmed. If the current area is not disarmed, then all authorized areas will be disarmed.
Cycle Output	Passcode + [ENTER] key will momentarily activate Enter Key Output for 10 seconds when a user enters a valid passcode and presses [ENTER] on the keypad.
Auto Re-Arm	Passcode + [ENTER] key will restart All On Delay Arm assigned to the keypad within the users authorized scope if the current area is not disarmed. If the area is disarmed, then the arm state does not change.
Login Only	Passcode + [ENTER] key will login the user.
Login/Disarm	Passcode + [ENTER] key will login the user and all armed areas within the users authorized scope will be disarmed.

This prompt defines a single purpose to this keypad; however entry of a passcode with authority in the current area will always silence alarms and troubles.
When a Passcode Enter Function is unable to be executed due to configuration conflicts or an unready device, then the control panel performs the Arm/Disarm function regardless of setting.
The D9412GV4and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
The Service Passcode (User ID 0) cannot be used to operate the Passcode Enter Functions.
When DUAL AUTHENTICATION is enabled, MENU 38 door control functions only work if **Passcode Enter Function** is set for Cycle Door.
Outputs used for the Cycle Output function must not be shared with any other point, sensor reset, control panel, or bell functions. Sharing can cause errors in output operation.
When performing the Cycle Door function, the door does not cycle if the Assign Door # parameter is not programmed.
When performing the Cycle Door function, "9210 NOT READY" appears at this Keypad if the door controller is busy, disabled or not configured correctly. ACCESS GRANTED appears if the function was successful.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set keep this parameter its default setting. Refer to SIA CP-01 Verification for more information.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Passcode Enter Function

Dual Authentication

Default: No
Selections: Yes / No
This parameter sets the requirement that a passcode must be entered at the keypad and a credential must be presented at the assigned door in order to gain access.
IMPORTANT
Before setting this parameter to Yes, first set Assign Door to Yes. If the Keypad Type is set to B94x Touch screen keypad, Assign Door can be either Yes or No.
Reference Keypads > SDI2 Keypad Assignments > Dual Authentication

Dual Authentication Duration

Default: 20 Seconds
Selections: 10, 15, 20, 25, 30, 35, 40, 45 seconds
This parameter sets the time out between the presentation of the door credential to the reader and the time the passcode is entered at the keypad.
Reference
Keypads > SDI2 Keypad Assignments > Dual Authentication Duration

Assign Door

Default: No Door
Selections:
D9412GV4: No Door, Door 1 to Door 8
D7412GV4: No Door, Door 1, Door 2

IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- A setting of No Door disables the Cycle Door option of KP# Passcode Enter Function.
- A setting of No Door disables the Add Card option of the Add/Change User command for this keypad.
- A setting of No Door disables KP# Dual Authentication for this keypad.

Enter the door number that is used by this command center for adding tokens/cards and displaying the KP# Close Door display.
9210 NOT READY appears at this keypad when you are attempting to add a user if a door is not entered in this parameter and a door is not assigned to the area using the D# Entry Area in the ACCESS CONTROL section. This indicates that access credentials cannot be assigned to a user through the ADD/CHANGE User command at this keypad until a door number is assigned.
A door does not need to be assigned to a keypad 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 door control authority enabled at a keypad with the doors area, assigned in the ACCESS CONTROL section, within its scope.
IMPORTANT: During the ADD USER? mode, token/cards, door control requests and RTE/REX do not function. If there is heavy activity for this door, set the door mode into an unlocked state before adding users.
No Door: No door controller is assigned for adding tokens or the CLOSE DOOR # display on the keypad.
1 - 8: Assign the door controller that enters the Add User? mode when initiated. This door activates the CLOSE DOOR # display at this keypad if KP# Close Door is set to Yes.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Assign Door

Trouble Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the panel wide trouble tones (power, phone, SDI bus and Zonex bus).
Panel wide trouble tones do not include point troubles, buzz on fault, or close door now.
Assign two keypad numbers to the same area to have one keypad sound the tone while another does not.

IMPORTANT:
- To meet UL864 requirements, set this parameter to **Yes**.
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

Yes: Panel wide trouble tones sound and visual displays show at this keypad.
No: Panel wide troubles do not sound. Visual displays still show.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Trouble Tone

Entry Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the DISARM NOW entry delay tone. Any delay point within the area scope of this keypad initiates the entry sequence.
This parameter allows you to manage the tone by keypad. Entry tone can also be turned off when programming your P## Ent Tone Off in Point Index.
Assign two KP#'s to the same area and have one KP# sound the tone while the other does not.
Yes: This keypad sounds entry tones.
No: This keypad does not sound entry tones.
Reference
Keypads > SDI2 Keypad Assignments > Entry Tone

Exit Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the EXIT NOW exit delay tone during the delay arming of an area(s). Any keypad that has a scope to arm this area can initiate the exit tone sequence.
This parameter allows you to manage the tone by keypad. Exit tone can also be turned off when programming your A# Exit Tone in Area Parameters.
Assign two KP#'s to the same area and have one KP# sound the tone while the other not.
Yes: This keypad sounds exit tones.

No: This keypad does not sound exit tones.
Reference
Keypads > SDI2 Keypad Assignments > Exit Tone

Arm Area Warning Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad sounds an audible tone and displays the PLEASE CLOSE NOW warning on the keypad when a closing window has activated.
Yes: This keypad activates a tone and display PLEASE CLOSE NOW.
No: This keypad does not activate the tone or display PLEASE CLOSE NOW.
Reference
Keypads > SDI2 Keypad Assignments > Arm Area Warning Tone

Close Door Warning Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad sounds an audible tone and displays the CLOSE DOOR # warning on the keypad when the door is physically held open past the Shunt Time, and Extend Time has a value greater than zero (see ACCESS CONTROL section) for the door assigned to this area in KP## Assign Door.
Yes: This keypad sounds a tone and display CLOSE DOOR #.
No: This keypad does not sound the tone or activate the display.
Reference
Keypads > SDI2 Keypad Assignments > Close Door Warning Tone

Idle Scroll Lock

Default: No (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
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.
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.
Reference
Keypads > SDI2 Keypad Assignments > Idle Scroll Lock

Function Lock

Default: No
Selections: Yes/No
This parameter determines if the Function Lock requires a passcode when pressed to access the functions.
Yes Pressing a function key (eg Menu, Bypass, Part, All) requires a passcode before proceeding.
No Pressing a function key does not require a passcode until a function requiring one is selected.
The user is prompted to enter a passcode after pressing the Function key on the keypad. The items programmed in the function List for this specific keypad are filtered by the user's authority level. Only those items in the function list for which the user has authority appear.
If set to No, when the user presses the Function key, all items that are programmed in the Menu List for the keypad address appear, regardless of the user's authority level.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Function Lock

Abort Display

Default: Yes (for all KP addresses)
Selections: Yes or No
Select whether or not the keypad shows `ALARM NOT SENT` if the alarm is aborted before an event report is sent to the central station.
IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **No**.

Yes: This keypad shows `ALARM NOT SENT` for all aborted alarms within its scope
No: This keypad does not show `ALARM NOT SENT` for all aborted alarms within its scope
Reference
Keypads > SDI2 Keypad Assignments > Abort Display

Cancel Display

Default: Yes (for all KP addresses)
Selections: Yes or No
Select whether or not the keypad shows `CANCEL RPT SENT` if a burglar alarm is canceled after the control panel sends a burglar alarm report to the central station. To show this message, Cancel Reports must be set to **Yes**.
IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **No**.

Yes: This keypad shows the `Cancel Report Sent` message for a canceled burglar alarm within its scope.
No: This keypad **does not** show the `Cancel Report Sent` message for a canceled burglar alarm within its scope.
Reference
Keypads > SDI2 Keypad Assignments > Cancel Display

Nightlight Enable

Default: No
Selections: Yes, No
Users with authority to change the keypad display can select whether or not to enable the nightlight feature on the keypad.
When set to Yes, The display backlight and key backlight (B92x, B93x) shall remain illuminated at the minimum level when the keypad is “Idle”.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Nightlight Enable

Nightlight Brightness

Default: 2
Selections: 0-6
0 = nightlight off
6 = highest setting
This parameter sets the brightness level for the backlight on the keypad display.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Nightlight Brightness

Silence Keypress Tone

Default: No
Selections: Yes/No
This parameter enables or disables the keypress acknowledgement tone on the keypad.
Yes Disable keypress acknowledgement tone. Keypad is silent when buttons are pressed.
No Enable keypress acknowledgement tone. Users hear a tone each time they press a button on the keypad.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Silence Keypress Tone

Show Date and Time

Default: No
Selections: Yes, No
Users with authority to change the keypad display can select whether or not the keypad displays the date and time.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Show Date and Time

Keypad Volume

Default: 7
Selections: 0-7
This parameter sets the volume level for the keypress acknowledgement tone on the keypad.
0 The minimum volume setting.
1-6 Increases or decreases keypress volume. The higher the number, the louder the tone.
7 The maximum volume setting.
Adjusting the keypad volume in this parameter does not affect the volume of high priority tones such as alarms which always sound at maximum volume.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Keypad Volume

Keypad Brightness

Default: 6
Selections: 1-6
This parameter sets the brightness level for the LED display on the keypad.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Keypad Brightness

Disable Presence Sensor

Default: No
Selections:
Yes Disable Presence Sensor.
No Enable Presence Sensor.
This parameter enables or disables the Presence Sensor on the keypad.
When enabled, the Presence Sensor detects motion within close proximity to the keypad and brightens a dimmed display as a user approaches.
Available for the B94x Touch screen keypads.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Disable Presence Sensor

Disable Token Reader

Default: Yes
Selections:
Yes Disable Token Reader.
No Enable Token Reader
This parameter enables or disables the Token Reader on the keypad.
Disable when the proximity reader is not in use with the system or if a door reader is used instead of a token reader. Disabling the token reader when not in use reduces power consumption. Available for the B94x Touch screen keypads.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Disable Token Reader

Enable Tamper Switch

Default: No
Selections:
Yes Enable the Tamper Switch.
No Disable the Tamper Switch.

RPS Menu Location
Keypads > SDI2 Keypad Assignments > Enable Tamper Switch

Card Type

Default: 26 bit
Selections:
– 26 bit
– 37 bit
This parameter specifies the card format used for all of the door controllers.
26 bit: Site Code will be set to 255.
37 bit: Site Code will be set to 0.
IMPORTANT
Changing this parameter erases all entries currently under Card Data, and Site Code fields returns to factory defaults.
Reference
Access Control > Door, Strike, and Event Profiles > Card Type

5.1.1 Global Keypad

A Key Response

Default: No Response
Selections:
No response Invalid key press tone.

Manual Fire Alarm B92x Two-line Keypad - When "A" key and 1 key are held together for 2 seconds.
B94x Touch Screen Keypad - When Fire key is held.
"A" Key Custom Function B92x Two-line Keypad only- When "A" key is held.

This parameter specifies how the control panel responds when the A Key is held on a B92x Two-line Keypad . The A Key and 1 key need to be held together for the Manual Fire Alarm selection. The parameter also enables the Fire emergency key for B94x Touch Screen Keypads.

For the Manual Fire Alarm selection, an alarm occurs each time the user presses the applicable keys whether or not the event has been cleared from the display. The panel sends a Fire alarm report in modem and contact ID. There are no restoral events for manual fire alarm events. No restoral reports are sent.

If this parameter is set to the Custom Function selection then the A Key Custom Function parameter must not be set to the Disabled selection. If it is, holding the "A" key sounds an Error tone.

RPS Menu Location:

Keypads > SDI2 Keypad Assignments > Global Keypads > A Key Response

A Key Custom Function

Default: Disabled

Selections:

- D9412GV4: Disabled, CF128 .. CF143
- D7412GV4: Disabled, CF128 .. CF131

This parameter specifies the custom function that is run when the A Key on a B920 series keypad is held for 2 seconds.

If this parameter is set to the Disabled selection, the keypad sounds an Error tone when the A Key is held.

The Custom Function selections shown for this parameter are defined in CUSTOM FUNCTIONS. If no Custom Function Text is assigned to the custom function, then the custom function number (CF###) appears in the list of selections here.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Global Keypad > A Key Custom Function

B Key Response

Default: No Response

Selections:

No Response	Invalid key press tone.
Manual Medical Alarm, no Alarm Output	B92x Two-line Keypad - medical alarm event when B Key and 1 key are held together for 2 seconds. B94x Touch Screen Keypad - medical alarm event when Medical key is held. No alarm output with alarm event.
Manual Medical Alarm with Alarm Output	B92x Two-line Keypad - medical alarm event when B Key and 1 key are held together for 2 sec. B94x Touch Screen Keypad - medical alarm event when Medical key is held. Alarm event turns on Summary Alarm output. Output turns off when alarm event is cleared from display.
"B" Key Custom Function	B92x Two-line Keypad only, when key is held the custom function selected in the B Key Custom Function parameter is run.

This parameter specifies how the control panel responds when the B Key is held on a B92x Two-line Keypad . The B Key and 1 key need to be held together for the Medical Alarm selection. The parameter also enables the Medical emergency key for B94x Touch Screen Keypads.

For the Manual Medical alarm selection, an alarm occurs each time the user presses the applicable keys whether or not the event has been cleared from the display. The panel sends a Medical alarm report in modem and contact ID. There are no restoral events for manual Medical alarm events. No restoral reports are sent.

If this parameter is set to the Custom Function selection then the "B" Custom Function parameter must not be set to the Disabled selection. If it is, holding the B key sounds an Error tone.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Global Keypads > B Key Response

B Key Custom Function

Default: Disabled

Selections:

- D9412GV4: Disabled, CF128 .. CF143
- D7412GV4: Disabled, CF128 .. CF131

This parameter specifies the custom function that is run when the B Key on a B920 series keypad is held for 2 seconds.

If this parameter is set to the Disabled selection, the keypad sounds an Error tone when the B Key is held.

The Custom Function selections shown for this parameter are defined in CUSTOM FUNCTIONS. If no Custom Function Text is assigned to the custom function, then the custom function number (CF###) appears in the list of selections here.

RPS Menu Location:

Keypads > SDI2 Keypad Assignments > Global Keypad > B Key Custom Function

C Key Response

Default: No Response

Selections:

No Response	Indicates an invalid key press tone.
Manual Panic Alarm, Invisible and No Alarm Output	B92x Two-line Keypad - Panic alarm event when C Key and 1 key are held together for 2 seconds. B94x Touch Screen Keypad - Panic alarm event when the Panic key is held. No indication in the keypad display and no alarm output with alarm event
Manual Panic Alarm, Visible with Alarm Output	B92x Two-line Keypad - Panic alarm event when C Key and 1 key are held together for 2 seconds. B94x Touch Screen Keypad - Panic alarm event when Panic key is held. Alarm event shows in display and turns on Summary Alarm output. Output turns off when alarm event is cleared from display.
"C" Key Custom Function	B92x Two-line Keypad only, when key is held the custom function selected in the C Key Custom Function parameter is run.

This parameter specifies how the control panel responds when the C Key is held on a B92x Two-line Keypad . The C Key and 1 key need to be held together for the Panic Alarm selection. The parameter also enables the Panic emergency key for B94x Touch Screen Keypads.

For the Manual Panic alarm selection, an alarm occurs each time the user presses the applicable keys whether or not the event has been cleared from the display. The panel sends an Hold-up alarm report in modem and contact ID. There are no restoral events for manual Hold-up alarm events. No restoral reports are sent.

If this parameter is set to the Custom Function selection then the C Key Custom Function parameter must not be set to the Disabled selection. If it is, holding the C Key sounds an Error tone.
RPS Menu Location:
Keypads > SDI2 Keypad Assignments > Global Keypads > C Key Response

C Key Custom Function

Default: Disabled
Selections:
– D9412GV4: Disabled, CF128 .. CF143
– D7412GV4: Disabled, CF128 .. CF131
This parameter specifies the custom function that is run when the C Key on a B920 series keypad is held for 2 seconds.
If this parameter is set to the Disabled selection, the keypad sounds an Error tone when the C Key is held.
The Custom Function selections shown for this parameter are defined in CUSTOM FUNCTIONS. If no Custom Function Text is assigned to the custom function, then the custom function number (CF###) appears in the list of selections here.
RPS Menu Location:
Keypads > SDI2 Keypad Assignments > Global Keypad > C Key Custom Function

Manual Silent Alarm Audible on Comm Trouble

Default: No
Selections: Yes/No
This parameter activates the Alarm Bell output and keypad sounders for the remaining Burg Bell time if a keypad or keyfob silent alarm fails in two attempts to transmit its report to the configured destination.
Yes Enable the Alarm Bell to activate when the silent alarm event fails to reach central station.
No Does not activate the Alarm Bell when the silent alarm event fails to reach central station.
This option only has an effect if a keypad's C key or a keyfob panic is configured to create a silent alarm.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Global Keypad Settings > Manual Silent Alarm Audible on Comm Trouble

5.2 SDI Keypad Assignments

Supervision

Default: No
Selections: Yes/No
Supervise this SDI address and generate `TROUBLE SDI ##` reports and local trouble annunciation if a problem occurs with this keypad or the SDI bus.
IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- Keypads sharing the same address setting display the same text and sound the same tones regardless of which keypad keys are being pressed.

- TROUBLE SDI # reports are always reported as Area 1, Account 1 events regardless to which area the SDI device is assigned.
- To meet UL864 requirements, set this parameter to **Yes** for the keypad used for fire annunciation.

Yes: Only one keypad can be installed for this KP# SDI address.

IMPORTANT: When this parameter is set to Yes, you cannot have duplicate DIP switch settings.

No: More than one keypad can be installed using this KP# SDI address using the same address DIP switch setting.

Reference

Keypads > SDI Keypad Assignments > Supervision

Enhanced keypad

Default: No

Selections: Yes/No

IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

Use this parameter to identify that a D1260 Series Keypad is installed at this address. You must reboot the control panel after enabling a D1260 Series Keypad. Reboot the control panel by checking the Reset Panel option when ending the RPS session.

Reference

Keypads > SDI Keypad Assignments > Enhanced Keypad

Area Assignment

Default: 1

Selections:

– D9412GV4: 1 to 32
– D7412GV4: 1 to 8

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

IMPORTANT:

– The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
– The D9412GV4 supports up to 32 areas and the D7412GV4 supports up to 8 areas.

Reference

Keypads > SDI Keypad Assignments > Area Assignment

Scope

Default:

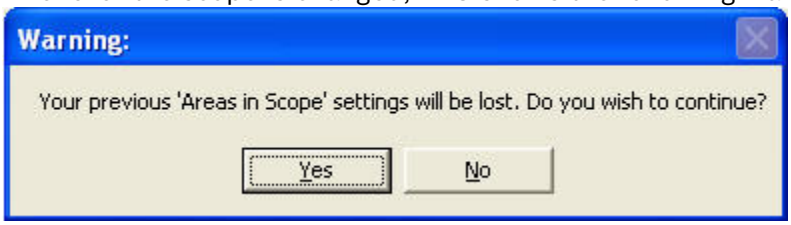
– KP Address 1 and 8: Panel Wide
– KP Addresses 2-7 and 9-16: No Keypad

Selections:

– No Keypad
– Area Wide
– Account Wide
– Panel Wide
– Custom

IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

Use this parameter to define what areas are affected when this keypad is armed, what areas can be viewed with this keypad, and what areas this keypad can move to. Whenever the scope is changed, RPS shows the following warning dialog:



– If you click **Yes**, RPS resets the Area(s) In Scope parameter.
– If you click **No**, no changes are made in RPS.

No Keypad: No keypad installed at this address. CALL FOR SERVICE displays indicating that this address is not being polled by the control panel.
Area Wide: An area keypad is restricted to the viewing information and arming/disarming functions for the area to which it is assigned.
Account Wide: An account keypad can view information, and perform arming and disarming functions for all areas that have the same A# Acct Number. This is normally used for an associate area. See A# Area Type for information on associate areas.
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.
Custom: A custom keypad has no keypad restrictions.

Reference

Keypads > SDI Keypad Assignments > Scope

Area(s) In Scope

Default:

– KP Address 1: All (Areas 1-8)
– All other KP Addresses: none

Selections:

– D9412GV4: 1 to 32
– D7412GV4: 1 to 8

IMPORTANT:

- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.

This parameter 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.

Reference

Keypads > SDI2 Keypad Assignments > Areas in Scope

Passcode Follows Scope?

Default: Yes
Selections: Yes/No

Use this parameter to determine whether this keypad follows Scope, or whether it only arms or disarms the area to which it is assigned. Users must have authority enabled in Passcode Arm and Passcode Disarm. This parameter does not affect the Function List arming and disarming parameters.

IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- You can use this parameter to create a group of account-wide keypads that arm only the area to which they are assigned, even if the user has a passcode with arming authority rights in all areas.

Yes: All On 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.

IMPORTANT:
- If the area to which this keypad is assigned is armed, entering a valid passcode disarms this area and all other areas assigned to the scope of this keypad.
- If the area to which this keypad is assigned is disarmed, entering a valid passcode disarms this area and all other areas assigned to the scope of this keypad.

No: Allows a user to view areas within the programmed scope, but only arm or disarm the area programmed in Area Assignment when a passcode is entered.

Reference

Keypads > SDI Keypad Assignments > Passcode Follows Scope

Enter Key Output

Default: 0 (for all KP addresses)

IMPORTANT: (grayed out) This field may only be modified if "Passcode Enter Function" is set to "Cycle Output"

Selections:
- D9412GV4: 0 to 128, A, B, C
- D7412GV4: 0 to 64, A, B, C

Enter the output number that momentarily activates for 10 seconds when a user enters a valid passcode and presses [ENTER] on the keypad. Two events might be generated when this function is used: Output ### Set with User ID and, Output ### Reset without User ID.

Entering a valid code and pressing [ENTER] silences the bell tone.

Use this parameter to provide a low-level access control strike on a door. This parameter does not shunt a point.

IMPORTANT:
- When programmed to activate a output, the keypad's [ENTER] key cannot be used for any other function. Outputs used for this function must not be shared with any other point, sensor reset, control panel or bell functions. Doing so can cause erroneous output operation.
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

0 (zero): The [ENTER] key is not used to cycle a output.

1 to 128, A, B, C: Assign the output number that activates when [ENTER] is pressed at this keypad after the user enters a valid passcode.

Reference

Keypads > SDI Keypad Assignments > Enter Key Output

Passcode Enter Function

Default: Arm/Disarm (all KP addresses)

Selections: Arm/Disarm, Cycle Output, Cycle Door, Auto Re-Arm.

Arm/Disarm: Passcode followed by ENTER (or ENT) key will start all on Delay Arm for all areas within the users authorized scope if the current area is disarmed. If the current area is not disarmed, then all authorized areas will be disarmed.

Cycle Output: Passcode followed by ENTER (or ENT) key will momentarily activate Enter Key Output for 10 seconds when a user enters a valid passcode and presses [ENTER] on the keypad.
Cycle Door: Passcode followed by ENTER (or ENT) key will cycle the door controller programmed in Assign Door # for the D# Strike Time duration, then will actuate the users authorized post access operations (Disarm, Part On Instant, or execute a Custom Function) if enabled.
Auto Re-arm: Passcode followed by ENTER (or ENT) key will restart all on Delay Arm assigned to the keypad (keypad) within the users authorized scope if the current area is not disarmed. If the area is disarmed, then the arm state does not change.
Setting this prompt defines a single purpose to this keypad; however entry of a passcode with authority in the current area will always silence alarms and troubles. When a Passcode Enter Function is unable to be executed due to configuration conflicts or an unready device, then the control panel performs the Arm/Disarm function regardless of setting.

IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- The Service Passcode (User ID 0) cannot be used to operate the Passcode Enter Functions.
- Outputs used for the Cycle Output function must not be shared with any other point, sensor reset, control panel, or bell functions. Sharing can cause errors in output operation.
- When performing the Cycle Door function, the door does not cycle if the Assign Door # parameter is not programmed.
- When performing the Cycle Door function, "9210 NOT READY" appears at this keypad if the door controller is busy, disabled or not configured correctly. ACCESS GRANTED appears if the function was successful.
- To comply with SIA CP-01 False Alarm Reduction, set keep this parameter its default setting. See SIA CP-01 Verification for more information.

RPS Menu Location
Keypads > SDI Keypad Assignments > Passcode Enter Function

Assign Door

Default: KP Address 1 = Door1, all other KP Addresses = No Door
Selections:
- D9412GV4: No Door, Door 1 to Door 8
- D7412GV4: No Door, Door 1, Door 2

IMPORTANT:
- This parameter only applies to the D9412GV4 and the D7412GV4 control panels.
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- A setting of No Door disables the Cycle Door option of KP# Passcode Enter Function.
- A setting of No Door disables the Add Card option of the Add/Change User command for this keypad.

Enter the door number that is used by this keypad for the Cycle Door passcode function or to show the Close Door warning.
No Door: No door controller is assigned to the keypad.
1 - 8: Assign the door controller that activates when the KP## Passcode Function is set to Cycle Door.
Reference
Keypads > SDI Keypad Assignments > Assign Door

Trouble Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the panel wide trouble tones (power, phone, SDI bus and Zonex bus).
Panel wide trouble tones do not include point troubles, buzz on fault, or close door now.
Assign two keypad numbers to the same area to have one keypad sound the tone while another does not.
IMPORTANT:
– To meet UL864 requirements, set this parameter to **Yes**.
– The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Yes: Panel wide trouble tones sound and visual displays show at this keypad.
No: Panel wide troubles do not sound. Visual displays still show.
Reference
Keypads > SDI Keypad Assignments > Trouble Tone

Entry Tone

Default: No (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the DISARM NOW entry delay tone. Any delay point within the area scope of this keypad initiates the entry sequence.
This parameter allows you to manage the tone by keypad. Entry tone can also be turned off when programming your P## Ent Tone Off in Point Index.
Assign two KP#'s to the same area and have one KP# sound the tone while the other does not.
Yes: This keypad sounds entry tones.
No: This keypad does not sound entry tones.
Reference
Keypads > SDI Keypad Assignments > Entry Tone

Exit Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this keypad or any keypad with the same address setting, sounds the EXIT NOW exit delay tone during the delay arming of an area(s). Any keypad that has a scope to arm this area can initiate the exit tone sequence.
This parameter allows you to manage the tone by keypad. Exit tone can also be turned off when programming your A# Exit Tone in Area Parameters.
Assign two KP#'s to the same area and have one KP# sound the tone while the other not.
Yes: This keypad sounds exit tones.

No: This keypad does not sound exit tones.
Reference
Keypads > SDI Keypad Assignments > Exit Tone

Arm Area Warning Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Use this parameter to determine whether this kaypad sounds an audible tone and displays the PLEASE CLOSE NOW warning on the keypad when a closing window has activated.
Yes: This keypad activates a tone and display PLEASE CLOSE NOW.
No: This keypad does not activate the tone or display PLEASE CLOSE NOW.
Reference
Keypads > SDI Keypad Assignments > Arm Area Warning Tone

Close Door Warning Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
IMPORTANT:
- This parameter only applies to the D9412GV4 and the D7412GV4 control panels.
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

Use this parameter to determine whether this keypad sounds an audible tone and displays the CLOSE DOOR # warning on the keypad when the door is physically held open past the Shunt Time, and Extend Time has a value greater than zero (see ACCESS CONTROL section) for the door assigned to this area in KP## Assign Door.
Yes: This keypad sounds a tone and display CLOSE DOOR #.
No: This keypad does not sound the tone or activate the display.
Reference
Keypads > SDI Keypad Assignments > Close Door Warning Tone

Abort Display

Default: Yes (for all KP addresses)
Selections: Yes or No
Select whether or not the keypad shows `ALARM NOT SENT` if the alarm is aborted before an event report is sent to the central station.
IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **No**.

Yes: This keypad shows `ALARM NOT SENT` for all aborted alarms within its scope
No: This keypad does not show `ALARM NOT SENT` for all aborted alarms within its scope
Reference
Keypads > SDI Keypad Assignments > Abort Display

Cancel Display

Default: Yes (for all KP addresses)
Selections: Yes or No
Select whether or not the keypad shows `CANCEL RPT SENT` if an alarm is canceled after the control panel sends an alarm report to the central station.
To show this message, Cancel Reports must be set to **Yes**.

IMPORTANT:
- The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **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.
Reference
Keypads > SDI Keypad Assignments > Cancel Display

Fire Keypad

Default: No
Selections:
Yes Select Yes to enable a Fire Keypad. Idle Scroll locks automatically.
No Select No when using a standard keypad.
This parameter enables the fire keypad. The keypad displays Alarm Silence? first in the fire menu when idle and the ESC key are pressed.
RPS Menu Location
Keypads > SDI Keypad Assignments > Fire Keypad

5.2.1 Area Text

"Area # Is On" Text

Default: A# AREA IS ON ("#" = Area number)
Selections: Blank or 16 alphanumeric characters
- Valid characters: A-Z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

Enter the text for this area that displays when the area is All On or All On Instant and there are other areas that share the same account number that are not yet All On. This display does not appear when the area is Part On.

IMPORTANT: The D9412GV4 supports up to 32 areas and the D7412GV4 supports up to 8 areas.

RPS Menu Location
Keypads > SDI Keypad Assignments > Area Text > "Area # is On" Text

"Area # Not Ready" Text

Default: A# NOT READY ("#" = Area number)
Selections: Blank or 16 alphanumeric characters
- Valid characters: A-Z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

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

IMPORTANT: The D9412GV4 supports up to 32 areas and the D7412GV4 supports up to 8 areas.

RPS Menu Location
Keypads > SDI Keypad Assignments > Area Text > Area # Not Ready Text

"Area # Is Off" Text

Default: A# AREA IS OFF ("#" = Area number)
Selections: Blank or 16 alphanumeric characters
- Valid characters: A-Z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

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

IMPORTANT: The D9412GV4 supports up to 32 areas and the D7412GV4 supports up to 8 areas.

RPS Menu Location
Keypads > SDI Keypad Assignments > Area Text > "Area # is Off" Text

"Area # Account Is On" Text

Default: A# ACCOUNT IS ON ("#" = Area number)
Selections: Blank or 16 alphanumeric characters
- Valid characters: A-Z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

Enter the text that displays when all areas sharing the same account number have been All On. The Acct Is On text appears at all keypads that are assigned to this area if more than one area has the same account number. The Acct Is On text also appears if only one area in the system is used. See Area Assignment and Account Number for more information.
When all areas in the account are All Oned, the Area # Is On text is replaced by the Account Is On text if the area was armed prior to all the areas with the same account number being armed.
Each area can have unique Account Is On text, or you can program the same text in each area of the account so that when all the areas in the account are armed, they all show the same text.

Although it is not programmed in this section, the D1260 keypad has the capability of displaying up to 16 characters for an Area Name on line 1 of its display. The Area Text (Area # is Off, Area # Not Ready, Area # is On, and Acct # is On) programmed in this section appears on line 2 of the D1260 keypad. Therefore, consideration should be given when programming this text so it makes sense to the end user when viewing it on the D1260. For example, the Area Name Text could be programmed to display Front Office and the Area # is Off text could be programmed to display Ready To Arm. The D1260 would then show Front Office on line 1 and Ready To Arm on line 2.

IMPORTANT: The D9412GV4 supports up to 32 areas and the D7412GV4 supports up to 8 areas.

RPS Menu Location

Keypads > SDI Keypad Assignments > Area Text > "Area # Account is On" Text

5.3 Wireless Keyfob

Keyfob Function A Custom Function Number

Default: Disabled

Selections:

- D9412GV4: Disabled, 128 - 143
- D7412GV4: Disabled, 128 - 131

This parameter specifies the custom function that is run when the Auxiliary Function B button is pressed on the key fob.

On the RADION four-button keyfobs, pressing the third button activates Auxiliary Function A. When the auxiliary function button is pressed, the control panel looks up the custom function configured in this parameter. If it is configured as disabled (0), then no action occurs.

When the custom function is run, it is executed as if the key strokes were entered on the configured keypad. The keyfob whose button is pressed identifies the user and no passcodes are required to run the custom function or to execute the commands in the custom function. The authority level configuration of the keyfob user governs whether the individual commands within the custom function execute. If the key fob user has no authority to run a command in the custom function, any remaining commands in the custom function abort.

RPS Menu Location

Keypads > Wireless Keyfob > Keyfob Function A Custom Function Number

Keyfob Function B Custom Function Number

Default: Disabled

Selections:

- D9412GV4: Disabled, 128 - 143
- D7412GV4: Disabled, 128 - 131

This parameter specifies the custom function that is run when the Auxiliary Function B button is pressed on the Key fob.

On the RADION four-button keyfobs, pressing the fourth button activates Auxiliary Function B. When the auxiliary function button is pressed, the control panel looks up the custom function configured in this parameter. If it is configured as disabled (0), then no action occurs.

When the custom function is run, it is executed as if the key strokes were entered on the configured keypad. The keyfob whose button is pressed identifies the user and no passcodes are required to run the custom function or to execute the commands in the custom function. The authority level configuration of the keyfob user governs whether the individual commands within the custom function execute. If the key fob user has no authority to run a command in the custom function, any remaining commands in the custom function abort.

RPS Menu Location

Keypads > Wireless Keyfob > Keyfob Function B Custom Function Number

Keyfob Panic Options

Default: Panic Response Disabled

Selections:

- Panic response disabled
- Audible panic response enabled
- Silent panic response enabled

This parameter activates the Area Wide Output alarm bell in each area that the keyfob user has authority when the panic button is pressed on any keyfob.

Panic response disabled The control panel ignores all panic button presses from every keyfob.

Audible panic response enabled The control panel generates an audible panic response when a panic button is pressed on any keyfob.

Silent panic response enabled The control panel generates a silent panic response when a panic button is pressed on any keyfob.

The keyfob panic response is enabled or disabled globally.

Audible Panic Response.

When an audible panic response is generated, the control panel logs a Keyfob Panic Alarm event. The user number associated with the keyfob is logged with the event. The outputs activate for the Burg Time configured in their respective areas. No alarm abort window is supported. A Burg Alarm is indicated and sounded on all keypads that have scope over the areas where the alarm bell is active.

Keyfob panic alarm events have a configuration option enabling or disabling their reporting by route group. This option is available only from RPS in PANEL WIDE PARAMETERS > Report Routing. This option controls the reporting of both Keypad Panic Alarms and Keyfob Panic Alarms.

Silent Panic Response.

When a silent panic response is generated, the control panel activates the Silent Alarm Output in each area that the keyfob user has authority. The outputs activate for the Burg Time configured in their respective areas. There is no indication or sound on any keypad. The control panel logs a Key Fob Silent Alarm event. The user number associated with the keyfob is logged with the event.

Keyfob silent alarm events have a configuration option, separate from the keyfob panic alarms, enabling or disabling their reporting by route group. This option is available only from RPS in PANEL WIDE PARAMETERS > Report Routing. This option controls the reporting of both Keypad Silent Alarms and keyfob Silent Alarms.

Reference

Keypads > Wireless Keyfob > Keyfob Panic Options

6 User Interface

6.1 Keypad Shortcuts

All On Delay

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This arming function allows a user to All On arm areas that are disarmed. If Enabled, the following arming choices are available to the user with this authority.
See below for an example of how these items are programmed and how it will affect the end user:
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > All On Delay

All On Instant

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This arming function allows a user to All On instant areas that are disarmed. If enabled, the arming choices below are available to the user with this authority.
IMPORTANT:
– Entry and Exit Delays **are not** provided with this arming function. This causes perimeter and interior delay points to act as instant points.
– To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Disabled (-)**. See SIA CP-01 Verification for more information.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > All On Instant

Part On Instant

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function Instant arms all Part On points that have a Pt Response that initiates an instant alarm (see Point Index) in the area where the Keypad is assigned.

IMPORTANT:
– Entry and Exit Delays **are not** provided with this arming function. This causes perimeter and interior delay points to act as instant points.
– To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Disabled (-)**. See SIA CP-01 Verification for more information.

Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Part On Instant

Part On Delay

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function Delay arms all Part On points in the area where the keypad is assigned. Entry and exit delays are provided with this arming function. *This will not cause a Part On instant point to act as a delay point.*
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Part On Delay

Watch Mode

Default: E (Enable)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function lets you know when a perimeter and interior point programmed as ***Watch Point*** has faulted while the point is disarmed. This function provides Keypad

audible/visual and optional output activation (see Watch Mode in the Area outputs section).
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Watch Mode

View Area Status

Default: P (Passcode)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to view the armed status of all areas within the scope of the keypad assigned to this area. The armed states include; AREA_#_IS_OFF (disarmed), AREA_#_IS ON (all on delay armed), ALL_ON_INSTANT (all on instant armed), and PART_ON (Part On instant armed or Part On delay armed). All area types (Master, Associate, Regular and Shared) can be viewed using this function.
IMPORTANT: The D9412GV4 and D7412GV4 support up to eight areas.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > View Area Status

View/Delete Event Memory

Default: E (Enable)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to view prior alarm, trouble, and supervisory activity that occurred since the last time the system was armed. Use this function to delete event memory as well.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > View/Delete Event Memory

View Point Status

Default: E (Enable)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user 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.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > View Point Status

Walk Test (All Non-Fire Burg Points)

Default: E (Enable)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user 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.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Walk Test (All Non-Fire Burg Points)

Walk test all fire points

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to test 24-hour points in areas within the Scope of the keypad where the function is entered. Controlled points, Type 1, 2, 3 , can not be tested using the fire walk test mode.
IMPORTANT: 24-Hour points left off-normal when exiting the Fire Test are bypassed. A trouble tone sounds until it is silenced. The keypads alternate text with the Bypass indications.

Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Walk Test All Fire Points

Send Report (Test/Status)

Default: E (Enable)
Selections:
- - (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to test the communication link between the panel and the central station receivers. It can send a test report or a status report to the phone numbers as programmed in Phone Routing. Reports can also be sent to an IP address, if programmed. The test report includes additional information if Expand Test Rpt is enabled in the Phone section.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Shortcuts > Send Report (Test/Status)

Set Keypad Brightness/Volume/Keypress

Default: E (Enable)
Selections:
- - (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to select either a bright or dim display with loud or soft keypad warning tones.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Set Keypad Brightness/Volume/Keypress

Set/Show Date and Time

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to set the time and date in the panel.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Set/Show Date and Time

Change Passcodes

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to change their passcode. This is a panel-wide function that can be executed from any keypad assigned to an area where the user has authority.
IMPORTANT: Regardless of whether an E or a P is placed here and Change Passcodes is performed, the keypad will prompt the user to enter their existing passcode first.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Change Passcodes

Add/Edit User

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows a user to add/change passcodes, add/change tokens/cards, and add/change panel authority levels (L##) by area.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.

Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Add/Edit User

Delete User

Default: P (Passcode)
Selections:
- - (Disabled)
- E (Enable)
- P (Passcode)

This function allows a user to delete a user's passcode and tokens/cards. It does not delete user names.
IMPORTANT: This function deletes the passcode, Master User associated with the user number.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Delete User

Extend Close

Default: P (Passcode)
Selections:
- - (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to change the expected closing time for the area. The window cannot be adjusted until the Close Early Begin time has passed and the closing window is active.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Extend Close

View Event Log

Default: E (Enable)
Selections:
- - (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to view all of the main events and the main event modifiers by user in the event log memory. User Name and Point Text are NOT stored in the event log but will appear when the panel matches them with the user ID ### and the point ### (respectively).
Each main event takes up one line in the log. Each modifier also takes up a line in the log.
The log in the panel can store 1024 events in the panel log.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > View Event Log

Bypass a Point

Default: P (Passcode)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to bypass individual points that are ***P## Bypassable***. Points within the Scope of the keypad can be bypassed where the function is entered (see Keypad Assignments).
The panel will ignore alarms/troubles and not display point faults when a point is bypassed.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Bypass A Point

Unbypass a Point

Default: P (Passcode)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This function allows the user to unbypass individual points that are programmed either P## FA Returnable or P## Bypass Returnable. Points within the Scope of the keypad can be unbypassed where the function is entered (see Keypad Assignments).
The panel will respond to alarms/troubles and display point faults when a point is unbypassed.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.

Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Unbypass a Point

Reset Sensors

Default: E (Enable)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to activate the Reset Sensors function for fire or intrusion points programmed as P## Resettable in the point index section. Points within the Scope of the keypad where the function is entered will be reset (see Keypad Assignments).
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Reset Sensors

Change Outputs

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to manually set and reset any outputs installed in the system.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
NOTE: The Change Outputs parameter also works with onboard points. Use the following output numbers to toggle the on-board outputs:
- Onboard Output A > Output #253
- Onboard Output B > Output #254
- Onboard Output C > Output #255

The D9412GV4 supports up to 128 outputs. The D7412GV4 supports up to 64 outputs.
RPS Menu Location
User Interface > Keypad Functions > Change Outputs

Remote Program

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to initiate RPS sessions. When the phone is ringing at the panel, the user initiates this function to have the panel seize the line.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Remote Program

Go to Area

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to temporarily switch the keypad's assignment to a different area. This 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 that the keypad is moved to. After fifteen (15) seconds of no activity at the keypad, the keypad reverts back to the originally programmed area.
IMPORTANT: The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8areas.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Go to Area

Display Panel Type and Revision

Default: E (Enable)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This function allows the user to show the panel's software revision number in the keypad display.

Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Display Panel Type and Revision

Service Walk All Points

Default: P (Passcode)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This function allows a user to walk test all points in the entire panel regardless of the point number or type.
IMPORTANT: 24-Hour points left off-normal when exiting the Service Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Shortcuts > Service Walk All Points

Change Skeds

Default: P (Passcode)
Selections:
- \- (Disabled)
- E (Enable)
- P (Passcode)

This is a panel-wide function that can be executed from any SDI2 keypad assigned to an area where the user has authority. This function allows the user to change the *Time* from the keypad to make adjustments to Skeds.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Change Skeds

Walk Test All Invisible Burg Points

Default: P (Passcode)
Selections:
– - (Disabled)
– E (Enable)
– P (Passcode)
This parameter allows a user with Invisible Walk Test authority to test invisible interior or perimeter controlled points that are within the scope of the keypad without sending a report to the central station.
Invisible points must have the Invisible Point parameter set to Yes.
IMPORTANT: 24-Hour points left off-normal when exiting the Invisible Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.
Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Enable (E): Enable the function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Walk Test All Invisible Burg Points

Custom Functions 128 to 143

Default: P (Passcode)
Selections:
– - (Disable)
– E (Enable)
– P (Passcode)
This function determines whether a passcode will be required (or not) when attempting to access a Custom Function from the Shortcut Menu, A-Key, B-Key, C-Key, or a Keyfob.
Disable (-): Disable the custom function panel wide.
Enable (E): Enable the custom function panel wide. The function can be performed without entering a passcode.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
The D9412GV2 supports 16 Custom Function 128-143. The D7412GV4 supports 4 Custom Functions 128-131.
RPS Menu Location
User Interface > Keypad Functions > Custom Functions 128 to 143

Keypad Programming

Default: P (Passcode)
Selections:
– - (Disabled)
– P (Passcode)
The control panel provides local keypad programming for a select list of parameters from B92x Two-line keypad and B93x ATM style keypads. Keypad programming is available in the Service Menu. Refer to the control panel documentation for more

information on keypad programming and the Service Menu. The Service Menu is not available on D1255 or D1260 series keypads.
Select whether this function is disabled (-), or if a passcode is required (P).

IMPORTANT:
- The Service Passcode is the only passcode that provides access to keypad programming.
- If at least one area is armed or the control panel is communicating with RPS, you cannot access keypad programming.

Disable (-): Disable the function panel wide. Accessing the function using the Function List displays **NO AUTHORITY**.
Passcode (P): Passcode required. When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Interface > Keypad Functions > Keypad Programming

6.2 Authority Levels

Disarm Select

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

Selections: Blank (-) or Enabled (E)
The disarming function allows a user to disarm areas that are All On or Part On. If enabled, the following disarming choices are available to the user with this authority.
- `DISARM ALL?`: Disarms all areas within the 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 area that is displayed.

There are many options available on how a user can arm and disarm. This is dependent upon Area Type and Scope.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Duress Disarm Profile
User Authority Level 14 is programmed by default as a Duress disarm profile. When Duress Type is set to **3**, the SIA CP-01 compliant Duress Passcode feature is enabled. Duress Types 1 and 2 are not allowed in SIA CP-01 compliant installations.
With Authority Level 14 assigned to a user passcode in an area, that user has the authority to disarm and send a Duress event from that area.
All Duress-capable passcodes must be unique and cannot be derived from other passcodes. To facilitate this uniqueness, User Authority Level 14 is pre-programmed from the factory as an example of Duress Disarm authority.
A Duress Disarm user authority level requires:
- Disarm (this parameter) set to **E**
- Send Duress set to **E**
- Passcode Disarm set to **E**

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference: User Interface > Authority Levels > Disarm Select

All On Delay

Default:
- **Authority Levels 1-5:** Enabled (E)
- **Authority Levels 6-15:** Blank (-)

Selections: Blank (-) or Enabled (E)

Arm all areas based on the scope of the keypad being used with an exit delay time. This parameter arms all perimeter and interior points within the scope of the keypad being used with an exit delay time in areas that correspond to the user's Authority Level.

If Command 1 is used, it arms only the area to which the keypad is assigned.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > All On Delay

All On Instant

Default:
- **Authority Levels 1 & 2:** Enabled (E)
- **Authority Levels 3-15:** Blank (-)

Selections: Blank (-) or Enabled (E)

This parameter arms all perimeter and interior points within the scope of the keypad being used with no exit delay time in areas that correspond to the user's Authority Level.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed. When All On Instant is accessed by entereing CMD 11/MENU 112, the area scope is restricted to the current area of the keypad.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > All On Instant

Part On Instant

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

Selections: Blank (-) or Enabled (E)

This parameter allows a user to arm all Part On points in areas that correspond to the user's Authority Level with no exit delay time.

When Part On Delay is accessed by entering CMD 3/MENU 121, the area scope is restricted to the current area of the keypad.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Part On Instant

Part On Delay

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

Selections: Blank (-) or Enabled (E)
This parameter allows a user to arm all perimeter points in areas that correspond to the user's Authority Level with exit delay.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Part On Delay

Watch Mode

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to initiate the watch mode in the area to which this keypad is assigned.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Watch Mode

View Area Status

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to view the current arm/disarm and not ready to arm status of all areas within the scope of the keypad in this area. The user must have arming/disarming authority.
IMPORTANT:
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.

- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > View Area Status

View Event Memory

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to view all memory events that have occurred since the last time the system was armed for all areas within the scope of the keypad in this area.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > View Event Memory

View Point Status

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

Selections: Blank (-) or Enabled (E)
This parameter allow the user with this authority level to view the current status of all points in the area to which this keypad is assigned.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > View Point Status

Walk Test (All Non-Fire burg Points)

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to initiate a walk test for all interior/perimeter controlled points in the area to which this keypad is assigned.

The following features are provided with the Walk Test Mode:
- During this test, the panel is being powered by the battery only. A battery test is initiated during the full duration of the test to ensure the battery capacity is capable of supporting the full load of the panel while AC is failed.
- This test includes an initial 2 second bell test when starting the walk test.
- The test ends once all points are tested or until the test times out in 20 minutes of no activity.
- Local alarm annunciation without reporting to the central station receiver.
- The keypad displays a sequential count after each point is activated and restored as well as the text for the point.

To walk test a door point, the door must be opened without activating the door sequence or allowed to time out past the extended shunt time.

IMPORTANT:
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
- 24-Hour points left off-normal when exiting the Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

RPS Menu Location

User Interface > Authority Levels > Walk Test (All Non-Fire Burg Points)

Walk Test All Fire Points

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to initiate a Fire walk test for all 24 hour points in the area to which this keypad is assigned.

When a Fire Test is initiated one person can typically test a fire system without assistance. The following features are provided with the Fire Test Mode:
- During this test, the panel is being powered by the battery only. A battery test is initiated during the full duration of the test to ensure the battery capacity is capable of supporting the full load of the panel while AC is failed.
- This test includes a two-second bell test (fire bell output) for each fire point that is tested.
- The test ends once all points are tested or until the test times out in 20 minutes of no activity.
- Local alarm annunciation without reporting to the central station receiver.
- Automatic smoke detector reset [SENSORS RESETTING] for all fire points programmed with P## Resettable as YES.
- The keypad displays a sequential count after each point is activated and restored as well as the text for the point.

IMPORTANT:
- Restart Time for fire points programmed with Alarm Verify as Yes is ignored during the Fire walk test.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

- 24-Hour points left off-normal when exiting the Fire Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Walk Test All Fire Points

Send Report (Test/Status)

Default:

- **Authority Levels 1 and 15:** Enabled (E)
- **Authority Levels 2-14:** Blank (-)

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to send a test report from any keypad assigned to an area where the user has authority.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Send Report (Test/Status)

Cycle Door

Default:

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to cycle a door from any keypad assigned to an area where the user has authority.

IMPORTANT:

- This parameter is only available on the D9412GV4 and D7412GV4 control panels.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Press the keypad number keys [1 through 8] that correspond to the door number to cycle doors. For example, pressing the 2 and the ENTER keys cycles door number 2, which is indicated by "C" in the display.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Cycle Door

(Un)lock Door

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

Selections: Blank (-) or Enabled (E)

IMPORTANT:
- This parameter is only available on the D9412GV4 and D7412GV4 control panels.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Press the keypad number keys [1 through 8] that correspond to the door number to unlock/relock doors. For example, pressing the 2 and the ENTER keys unlocks door number 2, which is indicated by "U" in the display.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Unlock Door

Secure Door

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

Selections: Blank (-) or Enabled (E)

IMPORTANT:
- This parameter is only available on the D9412GV4 and D7412GV4 control panels.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Press the keypad number keys [1 through 8] that correspond to the door number to secure/unsecure doors. For example, pressing the 2 and the ENTER keys secures door number 2, which is indicated by an "X" in the display.

This parameter allows the user with this authority level to secure a door from any keypad assigned to an area where the user has authority.

function.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Secure Door

Change Keypad Display

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to change the display (bright display, dim display, time display) in the area to which this keypad is assigned.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Change Keypad Display

Change Date and Time

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to change the date and time for the control panel in this area.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Change Date and Time

Change Passcodes

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to change a user passcode.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Change Passcodes

Add User Passcode/Card/Level

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to add/change users.
NOT READY appears if a door controller is not assigned, (see Assign Door) to the keypad being used to add/change tokens/cards.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Add User Passcode/Card/Level

Delete User Passcode/Card/Level

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority to delete users.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Delete User Passcode/Card/Level

Extend Close

Default: Service Walk
- **Authority Levels 1, 15:** Enabled (E)
- **Authority Levels 0, 2-14:** Blank (-)

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to change the closing time in the area where the function is entered.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Extend Close

View Event Log

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to view all panel wide events in the control panel's memory log.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > View Event Log

Bypass a Point

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to bypass points.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Bypass a Point

Unbypass a Point

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to unbypass points.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Unbypass a Point

Reset Sensors

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to reset sensors.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Reset Sensors

Change Outputs

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to set and reset outputs in the panel.
IMPORTANT:
- Do not use this parameter to toggle outputs reserved for special functions. Special function outputs are Area *and Panel Wide* output functions as well as outputs assigned to Enter Key Output.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Change Outputs

Remote Program

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

Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to initiate an RPS session when the phone rings at the control panel.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Remote Program

Go to Area

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to temporarily switch to a different area and perform keypad functions related to the area to which the keypad is switched.

IMPORTANT:
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Go to Area

Display Panel Type and Revision

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

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to display the control panel firmware revision.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

Reference

User Interface > Authority Levels > Display Panel Type and Revision

Service Walk All Points

Default:
- **Authority Levels 1, 15:** 1, Enabled (E)
- **Authority Levels 0, 2-14:** Blank (-)

Selections: Blank (-) or Enabled (E)

This parameter allows the user with this authority level to initiate a service walk test for all 24 hour interior/perimeter controlled points in the panel.

Points will not be included in this test if points are in an area that is already in any walk test mode, points are assigned to an area that is not enabled (Area On), or points are in an area that is all on or Part On.

When a Service Walk Test initiated, one person can test all the points in the panel without assistance. The following features are provided with the Service Test Mode:
- Display tells you exactly how many points can be tested.
- A Battery and Bell test does not occur during this walk test.

– The test ends once all points are tested or until the test times out in 20 minutes of no activity.
– The keypad displays a sequential count after each point is activated and restored as well as the text for the point.

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.

IMPORTANT:
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
- 24-Hour points left off-normal when exiting the Service Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Service Walk All Points

Change Skeds

Default:
– **Authority Levels 1, 15:** Enabled (E)
– **Authority Levels 2-14:** Blank (-)
Selections: Blank (-) or Enabled (E)
This parameter allows the user with this authority level to change skeds that can be edited.
Skeds can be restricted from being edited by setting Time Edit to No.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Change Skeds

Walk Test All Invisible Burg Points

Default:
– **Authority Levels 1, 15:** Enabled (E)
– **Authority Levels 2-14:** Blank (-)
Selections: Blank (-) or Enabled (E)
This parameter allows the user to test all points that are programmed to be invisible and that are within the scope of the keypad without sending a report to the central station.
This parameter allows a user with this authority level to start an invisible walk test for all 24-hour interior and exterior controlled points in the area to which this keypad is

assigned. The user does not need help from another person to conduct an invisible walk test.
Invisible points must have the Invisible Point parameter set to Yes.
The Invisible Walk test provides the following features:
– The display indicates exactly how many invisible points are assigned to the area.
– A battery and bell test does not occur during this test.
– The keypad displays point text when invisible points are tested.
– The test ends when all points are tested, or until the test times out after ten minutes of no activity.
– The keypad displays a sequential count and text related to the point after each point is activated and restored.
– Walk Test and Walk End reports are sent to the central station receiver for the beginning and end of the test (if programmed in routing).

IMPORTANT:
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
- 24-Hour points left off-normal when exiting the Invisible Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads will alternate text with the Bypass indications.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Walk Test All Invisible Burg Ponts

Custom Functions 128 to 143

Default:
– **Authority Level 1:** Enabled (E)
– **Authority Levels 2-15:** Blank (-)
Selections: Blank (-) or Enabled (E)
Allow the user with this authority level to execute the desired Custom Function.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
WARNING: The user authority to execute a Custom Function automatically grants the user authority to execute all commands within the programmed Custom Function. If a user does not have authority to do a specific command through the keypad menu, then it does not prohibit them from using the same command through a Custom Function.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
The D9412GV4 supports Custom Functions 128 through 143. The D7412GV4 supports Custom Functions 128 through 131.
Reference
User Interface > Authority Levels > Custom Functions 128 to 143

Force Arm

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

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to force arm the control panel.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Force Arm

Send Area Opening/Closing

Default:
- **Authority Levels 1 - 14:** Enabled (E)
- **Authority Level 15:** Blank (-)

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to generate opening and closing reports if the area to which this authority level is assigned sends opening and closing reports.
IMPORTANT:
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Send Area Opening/Closing

Restricted Open/Close

Default: Blank (-) for all authority levels
Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to initiate an opening report if a bell is ringing or a closing report when force/bypass arming. The area to which this authority level is assigned must be programmed for restricted openings and closings (see Restricted O/C).
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Restricted Open/Close

Part On Open/Close

Default:
- **Authority Levels 1 - 14:** Enabled (E)
- **Authority Level 15:** Blank (-)

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to report Part On opening and closing reports if the area to which this authority level is assigned sends Part On opening and closing reports.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
RPS Menu Location
User Interface > Authority Levels > Part On Open/Close

Send Duress

Default:
- **Authority Level 1-13, 15:** Blank (-)
- **Authority Levels 14:** Enabled (E)

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to send duress report if the area to which this authority level is assigned sends duress. See Duress Enable for more information.

IMPORTANT:
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
- Configure the Duress Enable parameter to **Yes** in applicable areas, or the keypad will respond with *No Authority*.

Duress Disarm Profile
User Authority Level 14 is programmed by default as a Duress disarm profile. When Duress Type is set to **3**, the SIA CP-01 compliant Duress Passcode feature is enabled. Duress Types 1 and 2 are not allowed in SIA CP-01 compliant installations.
With Authority Level 14 assigned to a user passcode in an area, that user has the authority to disarm and send a Duress event from that area.
All Duress-capable passcodes must be unique and cannot be derived from other passcodes. To facilitate this uniqueness, User Authority Level 14 is pre-programmed from the factory as an example of Duress Disarm authority.
A Duress Disarm user authority level requires:
- Disarm set to **E**
- Send Duress (this parameter) set to **E**
- Passcode Disarm set to **E**

- (Blank): 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.
Reference
User Interface > Authority Levels > Send Duress

Arm by Passcode

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

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to arm an area by entering their passcode, then pressing the [ENTER] key.
IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Arm by Passcode

Disarm by Passcode

Default:
- **Authority Levels 1-5 and 14:** Enabled (E)
- **Authority Levels 6-13 and 15:** Blank (-)

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to disarm an area by entering their passcode, then pressing the [ENTER] key.
IMPORTANT:
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
- Configure the Duress Enable parameter to **Yes** in applicable areas, or the keypad will respond with *No Authority*.

Duress Disarm Profile
User Authority Level 14 is programmed by default as a Duress disarm profile. When Duress Type is set to **3**, the SIA CP-01 compliant Duress Passcode feature is enabled. Duress Types 1 and 2 are not allowed in SIA CP-01 compliant installations.
With Authority Level 14 assigned to a user passcode in an area, that user has the authority to disarm and send a Duress event from that area.
All Duress-capable passcodes must be unique and cannot be derived from other passcodes. To facilitate this uniqueness, User Authority Level 14 is pre-programmed from the factory as an example of Duress Disarm authority.
A Duress Disarm user authority level requires:
- Disarm set to **E**
- Send Duress set to **E**
- Disarm by Passcode (this parameter) set to **E**

Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.
Reference
User Interface > Authority Levels > Disarm by Passcode

Security Level

Default:
- **Authority Levels 1, 2:** All On (A)
- **Authority Levels 3-5:** Part On (P)
- **Authority Level 6:** Disarmed (D)
- **Authority Levels 7-15:** No Access (-)

Selections:
- All On (A)
- Part On (P)
- Disarmed (D)
- No Access (-)

When the user presents a token/card at the reader, access is granted only when the user has the authority to enter the area under certain armed conditions.

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

All On (A): Users have access rights for this area when the area in any armed state.
Part On (P): Users have access rights for this area when the area is Part On or disarmed, but not when the area is all on Armed.
Disarmed (D): Users have access rights for this area only when it is disarmed.
No Disarm Rights (-): Users do not have access rights to this area.
RPS Menu Location
User Interface > Authority Levels > Security Level

Disarm Level

Default:
- **Authority Levels 1-5:** Disarm (D)
- **Authority Levels 6-15:** No Disarm Rights (-)

Selections:
- All or Part On to Part On Instant (I)
- Disarm (D)
- No Disarm Rights (-)

When the user presents a card door reader, the panel checks the Access Level and enables area disarm functions as programmed.
Opening and Closing reports are sent to the central station receiver if programmed.
For more information on programming this prompt for a Shared area, see the Access Control Readers Assigned to the Shared Area paragraph for the Area Type prompt in Area Parameters.

IMPORTANT:
- Burglar bells are silenced in the local area when a user disarms with a token/card, or presents the token/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/card has silenced the bell.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

All or Part On to Part On Instant (I): Users change the All On state and Part On state to [Part On INSTANT]. The armed state does not change in other areas, and the armed state does not change if the area is already in the Part On instant or disarmed state. User must have Access Level for All On (M) state.
Disarm (D): Users change the local area's All On state and Part On state to the disarm state. User must have Access Level for All On (M) or Part On (P) state. All areas

within the scope of the keypad assigned to the KP# Scope in the Access handler and areas to which the user has disarm rights disarm as programmed.
No Disarm Rights (-): Users do not have disarm rights in this area.
RPS Menu Location
User Interface > Authority Levels > Disarm Level

Function Level

Default:
- **Authority Level 1:** Disarmed (D)
- **Authority Levels 2-15:** No Function Level (-)

Selections:
- All On (A)
- Disarmed (D)
- All On and Disarmed (C)
- No Function Level (-)

All On (A): Activate the custom function assigned to the door in this area when the area is All On or Part On.
Disarmed (D): Activate the custom function assigned to the door in this area when the area is disarmed.
All On and Disarmed (C): Users can activate the custom function assigned to the door in this area regardless of the area's arming state.
No Function Level (-): Users cannot activate a custom function in this area.

IMPORTANT:
- When a token or card can also disarm an area, the custom function starts after the area disarms.
- A user does not require Security Level or Disarm Level authority to activate a custom function with a token or card.
- Tokens or cards that are used to execute custom functions must have a passcode assigned to the corresponding user.
- Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

User Interface > Authority Levels > Function Level

Keyfob Arm

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

Selections: Blank (-) or Enabled (E)
Allow a user with this authority level to arm an area by using their assigned keyfob.

IMPORTANT: 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 (-).

Duress operation when disarming is not applicable when using keyfobs.
Blank (-): This function is not authorized for the user who is assigned this authority level.
Enabled (E): This function is authorized for the user who is assigned this authority level.

IMPORTANT:
When upgrading from control panel firmware v2.00 or v2.01 to firmware versions 2.02 or newer, the Keyfob Arm/Disarm permissions in the prior versions are only carried over to the Keyfob Arm parameter. You must manually set the Keyfob Disarm parameter.

Reference

User Interface > Authority Levels > Keyfob Arm

Keyfob Disarm

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

Selections: Blank (-) or Enabled (E)

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

IMPORTANT: 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 (-).

Duress operation when disarming is not applicable when using keyfobs.

Blank (-): This function is not authorized for the user who is assigned this authority level.

Enabled (E): This function is authorized for the user who is assigned this authority level.

IMPORTANT

When upgrading from control panel firmware v2.00 or v2.01 to firmware versions 2.02 or newer, the Keyfob Arm/Disarm permissions in the prior versions are only carried over to the Keyfob Arm parameter. You must manually set the Keyfob Disarm parameter.

Reference

User Interface > Authority Levels > Keyfob Disarm

Firmware Update

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

Selections: Blank (-) or Enabled (E)

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

IMPORTANT: Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.

Reference

User Interface > Authority Levels > Firmware Update

7 Custom Function

Custom Functions -- Overview

Custom Functions are a way to simplify use of complex keystroke sequences that can be entered at the keypad. These items are similar to "speed dialing" on a telephone – in other words, a custom function can automatically initiate an end user request with one push of the ENTER key once the custom function text is displayed on the keypad. You can have up to 16 Custom Functions and restrict the use of these by area and authority level.
Each Custom Function ### item has an 18 character programmable text. When the custom function is assigned to the Shortcut Menu Function the user can user the PREV or NEXT key to scroll to the Custom Function Text.
The user must have the appropriate authority level enabled for the Custom Function 128-143 in the User Interface section, to be capable of using the custom function.

Custom Function Text

Default: Function #
Selections:
This entry determines the menu text displayed at the keypad for the Custom Function item. Use up to 32 valid characters to represent the functions performed by this menu item.
Reference
Custom Function > Custom Function Text

Function 1-6

Default: Not in Use
Selections: Refer to the list below.
This parameter sets the type of function to be used as a custom function.
Double-clicking in the Function # entry field displays the universal dialog box. Select a custom function from the list.

IMPORTANT
Please note that the control panel runs custom functions consecutively with each function in the list starting immediately after the previous function has begun and without waiting for a previous function to finish. If you program the control panel to run a function with a delay time, the next function in the list might result in unexpected behavior. In order to prevent this situation, you must program a "Delay" function between the two custom functions.
For example: To toggle an output at the end of a Part On Delay with a 30 second exit delay, set Function 1 to "Part On Delay", set Function 2 to "Delay" with a setting greater than 30 seconds, and set Function 3 to "Toggle Output".

FUNCTION:

Not in Use
This function is disabled and no functions after this will be performed.

All On Delay
This function emulates the "{function name}" shortcut keypad function. Entries in the Parameter 1:Area # prompt define the area(s) this function arms. If any point is faulted when the function executes, it is force armed regardless of the A## Force Arm Bypass Max setting.

All On Instant

This function emulates the "{function name}" shortcut keypad function. Entries in the Parameter 1:Area # prompt define the area(s) this function arms. If any point is faulted when the function executes, it is force armed regardless of the A## Force Arm Bypass Max setting.

Part On Delay

This function emulates the "{function name}" shortcut keypad function. Entries in the Parameter 1:Area # prompt define the area(s) this function arms. If any point is faulted when the function executes, it is force armed regardless of the A## Force Arm Bypass Max setting.

Part On Instant

This function emulates the "{function name}" shortcut keypad function. Entries in the Parameter 1:Area # prompt define the area(s) this function arms. If any point is faulted when the function executes, it is force armed regardless of the A## Force Arm Bypass Max setting.

Disarm

This function simulates the Disarm shortcut keypad function. Entries in the Parameter 1:Area # prompt define the area(s) this function disarms.

Extend Close

This function emulates the Extend Close shortcut keypad function. When this function is activated, all active closing windows in the areas selected in Parameter 1: Area # are extended from the time of activation plus the number of minutes configured in Parameter 2:Minutes #. This function cannot extend the closing time past midnight nor can it extend past an areas configured Latest Closing time.

Bypass a Point

This function emulates the Bypass Point shortcut keypad function. The entry in the Parameter 1: Point # prompt defines the point this function 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 Report Bypass at Occurrence is set to Yes by the point index settings assigned to the point. This function can only bypass one point.

Unbypass a Point

This function emulates the Unbypass Point shortcut keypad function. The entry in the Parameter 1: Point # prompt defines the point this function unbypasses. This function can only bypass one point.

Unbypass all Points

This function is not available as a shortcut keypad function. The areas selected in the Parameter 1: Area # prompt define the areas where this function unbypasses all points.

Reset Sensors

This function emulates the keypad shortcut Reset Sensors. When activated, this function activates the area-wide-output Reset Sensors for 5 seconds.

Turn Output On

This function emulates the Change Output State keypad shortcut to turn outputs on. The entry in the Parameter 1: Output # prompt defines the specific output this function activates. The function can activate one output.

Turn Output Off

This function emulates the Change Output State keypad shortcut to turn outputs off. The entry in the Parameter 1: Output # prompt defines the specific output this

function deactivates. The function can deactivate one output.

Toggle Output

This function is not available as a keypad shortcut function. The entry in the Parameter 1: Output # prompt defines the specific output this function toggles. If the output is on, it is turned off. If the output is off, it is turned on. The function has effect on one output.

One-Shot Output

This function is not available as a keypad shortcut function and is only available as a custom function. The entry in the Parameter 1: Output # prompt defines the specific output this function activates for the duration of time specified in Parameter 2: Seconds.

Reset All Outputs

This function is not available as a keypad shortcut function. This function turns off all outputs that are turned on by a sked or custom function. This is a panel-wide function. No other parameters require input for this option.

Delay

This function is not available as a keypad shortcut function and is only available in a custom function. This function pauses the execution of a custom function for the amount of time programmed in Parameter 1: Seconds.

Cycle Door

This function emulates the Cycle Door keypad shortcut function and is only available in a Custom Function. This function momentarily unlocks the door(s) programmed in Parameter 1: Door #.

Unlock Door

This function emulates the Unlock Door keypad shortcut function. This function unlocks the door(s) programmed in Parameter 1: Door #.

Lock Door

This function emulates the Lock Door keypad shortcut function. This function returns the door(s) programmed in Parameter 1: Door # to their normal locked state.

Secure Door

This function emulates the Secure Door keypad shortcut function. This function puts the door(s) programmed in Parameter 1: Door # in the Secured state which prohibits all access.

Access Control Level

This function is not available as a keypad shortcut function and determines whether a user's token or card authority level for access is enabled or disabled. When Parameter 1: Access Level is set to On, the authority levels programmed in Parameter 2: Level are granted access. When Parameter 1: Access Level is set to Off, the authority levels programmed in Parameter 2: Level are denied access.

Access Granted Events

This function is not available as a keypad shortcut function and determines whether access granted events are saved in the control panels event log. When Parameter 1: Access Level is set to On, the doors programmed in Parameter 2: Door # will put their access granted events in the control panel event log. When Parameter 1: Access Level is set to Off, the doors programmed in Parameter 2: Door # will not put their access granted events in the control panel event log.

Access Denied Events

This function is not available as a keypad shortcut function and determines whether access denied events are saved in the control panels event log. When Parameter 1: Access Level is set to On, the doors programmed in Parameter 2: Door # will put their access denied events in the control panel event log. When Parameter 1: Access Level is set to Off, the doors programmed in Parameter 2: Door # will not put their access denied events in the control panel event log.

Answer RPS

This function emulates the keypad short cut Answer RPS which causes the control panel to answer the next request from RPS to establish a session via phone or network. This function is only available in a custom function.

Contact RPS

This function emulates the keypad shortcut Contact RPS which attempts to contact an Unattended RPS via phone or network. The control panel's account in RPS controls the operations performed upon successful contact.

Contact RPS User Port

This function emulates the keypad shortcut Contact RPS user Port which attempts to contact an Unattended RPS via network at the port number programmed in Parameter 1: Port Number. The control panel's account in RPS controls the operations performed upon successful contact.

Send Test on Off-Normal

This function is not available as a keypad shortcut. When activated, this function check the control panel for any off-normal points or system troubles and sends a single test report to the central station with a summary of off-normal panel-wide status information. If the system is normal, then no test report is sent.

Go to Area

This function emulates the Go To Area keypad shortcut and is only available to custom functions activated through a keypad. When activated, this function will change the keypads current area to the one programmed in Parameter 1: Area #.

Watch On

This function emulates the operation of the keypad shortcut Change Watch Mode by activating Match mode for the areas programmed in Parameter 1: Area #. Watch mode causes a chime at any keypad within scope when a watch point is faulted while disarmed.

Watch Off

This function emulates the operation of the keypad shortcut Change Watch Mode by deactivating Match mode for the areas programmed in Parameter 1: Area #.

Show Date & Time

This function emulates the keypad shortcut Show Date & Time by displaying the current time and date at the SDI2 keypads specified in Parameter 1: Keypads #.

Sound Watch Tone

This function is not available as a keypad shortcut. When activated, this function causes the SDI2 keypads specified in Parameter 1: Keypads # to continuously emit a watch beep until silenced.

Set Keypad Volume

This function emulates the Keypad Volume keypad shortcut. When activated, this function sets the SDI2 keypad specified in Parameter 1: Keypad # to the volume level set in Parameter 2: Volume Level. This function only has effect on a single SDI2 keypad.

Set Keypad Brightness

This function emulates the Keypad Brightness keypad shortcut. When activated, this function sets the brightness level of the SDI2 keypad specified in Parameter 1: Keypad # to the level specified in Parameter 2: Brightness Level. This function only has effect on a single SDI2 keypad.

Trouble Silence

This function is not available as a Keypad Shortcut, but can be performed at any keypad through other means. When activated, this function silences all trouble tones and system buzzes in the areas programmed in Parameter 1: Area #.

Alarm Silence

This function is not available as a Keypad Shortcut, but can be performed at any keypad through other means. When activated, this function silences all alarms in the areas programmed in Parameter 1: Area #.

Reference

Custom Function > Function 1-6

8 Shortcut Menu

Function

Default:
- Menu 1: All On Select Area
- Menu 2: Off Selected Area
- Menu 3: View Point Status
- Menu 4: Reset Sensors
- Menu 5: Change Watch Mode
- Menu 6: Keypad Brightness
- Menu 7: Keypad Volume
- Menu 8: View Log
- All other menus: Disabled Item

Selections: (See chart below)
Select the function from the list below and next to the function in the User Interface section.
Function numbers 128 to 143 are custom functions and display the text programmed for Custom Function Text.
There is no restriction on how many times you may assign a specific function to the menu. By doing so, you can assign the same function at different keypads so they appear differently in some areas than they would in others.

Functions	Functions
Disabled Item	Change Passcode
All On Delay	Add User
All On Instant	Edit User
All On Select Area	Delete User
Part On Delay	Change Watch Mode
Part On Instant	Set Panel Date
Part On Select Area	Set Panel Time
Off	Show Date/Time
Off Select Area	Change Skeds
Extend Close	Keypad Brightness
Bypass a Point	Keypad Volume
Unbypass a Point	Silence Key Tone
View Area Status	View Event Memory
View Point Status	Delete Event Memory
Send Status Report	View Log
Reset Sensors	A Key Alarm (Fire)
Change Output State	B Key Alarm (Medical)
Fire Walk Test	C Key Alarm (Silent/Panic)
Intrusion Walk Test	CF 128

Functions	Functions
Service Walk Test	CF 129
Invisible Walk Test	CF 130
Send Test Report	CF 131
Display Revisions	CF 132
RPS Answer	CF 133
RPS via Network	CF 134
RPS via Network, Change Port	CF 135
RPS via Phone	CF 136
Go to Area	CF 137
Update Firmware	CF 138
View Service Bypassed	CF 139
Cycle Door	CF 140
Unlock Door	CF 141
Lock Door	CF 142
Secure Door	CF 143

Reference
Shortcut Menu > Function

Set/Clear All

Default: Set/Clr all
Selections: KP Address 1-16
Use this parameter to quickly enable or disable a selected function number at all available keypad addresses.
Any changes you make in the **Set/Clear All** window also appear in the specific KP Address cell. For example, if you check the boxes for KP Address 1 and KP Address 2 in the **Set/Clear All** window, the cells for KP Address 1 and KP Address 2 change to show **Yes**.
If you change any of the KP Address cells individually, those changes are appear in the **Set/Clear All KP** window.
IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).
Reference
Function List > Set/Clear All

Address

Default:

- **Menu Item 1-8**: Yes (all KP addresses)
- **Menu Items 9- 32:** No (all KP addresses)

Selections: Yes/No

This parameter determines at which keypad address setting this menu item appears. Any changes you make in the Set/Clear All KP window also appear in the specific KP Address cell. For example, if you check the boxes for KP Address 1 and KP Address 2 in the **Set/Clear All KP** window, the cells for KP Address 1 and KP Address 2 change to show **Yes**.

If you change any of the **KP Address** cells individually, those changes are appear in the **Set/Clear All KP** window.

IMPORTANT: The D9412GV4 and D7412GV4 support up to 16 keypads (KP Addresses 1 to 16).

Yes: This menu item appears at this keypad address.

No: This menu item does not appear at this keypad address.

Reference

Function List > Address

9 Output Parameters

Output Parameters Overview

Outputs provide dry contact (normally open/closed) outputs for LED annunciation and other applications as well as wet (12vdc on/off) voltage outputs for basic alarm system functions (such as Bell output, Reset Sensors, etc.). The applications are endless, but primarily, outputs are used to enhance a systems capability to perform output functions.

Output Types

- Panel Wide Outputs: These outputs are used to provide an output related to a "panel wide" indication. For annunciation, these outputs can be used to indicate "system wide" troubles for power, phone and overall panel summary of alarms, troubles and supervisory conditions.
- Area Outputs: These outputs are used to provide an output "by the area" that the output is assigned to. An area can have its own bell and sensor reset indications. Outputs can also be used to indicate the area armed state and whether any off normal conditions such as a force arm have occurred.
- On Board Outputs: There are 3 on board 12VDC voltage-outputs which provide power when activated on the panel. These outputs are default programmed from the factory as outputs A, B and C. Typically, output A is used for the Bell, output B is used for an alternate alarm output (such as another bell) and output C is used for Sensor Reset.
- Off Board Outputs: The panel can also control as many as 128 (for the D9412GV4) or 64 (for the D7412GV4) dry contact form "C" outputs when up to 16 D8129 or up to 12 B308 OctoOutput Modules are installed. These outputs are used for Area Output, Panel Wide Output, and Individual Point Fault Outputs.

Output Follows Point

Outputs can also be used to activate when a point programmed for, Rly Resp Type (in the point index section), is off normal or in alarm condition.

Output Reports

When output activity is reported to the receiver (see Phone Routing), on-board outputs are reported as follows: A = 253, B = 254, C = 255, and others report as 0001 to 0128. Output reports are also stored in the panel memory log.

Controlling Outputs

As mentioned, outputs can be activated depending upon conditions that exist with the panel. In addition, outputs can be controlled by the user using the [CHG OUTPUT?] function, Output On/Output Off skeds, and the RPS.

The following programming tips, notes and applications are important for you to review prior to programming your outputs.

IMPORTANT: Do not attempt to use the CHANGE OUTPUTS function to toggle outputs reserved for special functions. Special function outputs are Area and Panel Wide output functions as well as outputs assigned to Entr Key Rly and Rly Resp Type? .

Output C is always powered ON. Assigning any other output deactivates Output C so this output can be used for other functions. When Output C is programmed for Reset Sensors , power is always supplied from the AUX terminal of the panel.

Check output status after reprogramming or resetting the panel. All outputs are turned off after the panel is reset. Certain output functions are checked by the panel

each minute and will resume the correct state after the reset. Other outputs must be manually set to the correct state using the Change Output function (MENU 32).

These output functions resume the proper state within one minute:			
Alarm Bell	Fire Bell	Area Faul	Part On Fault
Battery Trouble	Summary Fire	Summary Alarm	AC Fail
Summary Fire Trouble	Summary Trouble	Phone Fail	Communications Fail
Area Armed	Silent Alarm	Watch Mode	Reset Sensors
Summary SupBurg	Summary SupFire		

These outputs functions need to be manually reset with Change Output function:	
Fail to Close	Force Armed
Duress	Log % Full

9.1 Area Wide Output

Alarm Bell

Default: A
Selections:
- D9412GV4: Blank, 0 to 128, A, B or C
- D7412GV4: Blank, 0 to 64, A, B or C

This output activates when an intrusion point assigned to this area goes into alarm. It will also activate for (non-fire) keypad and keyfob alarms that are configured to sound the Alarm Bell.
Burg Time and Burg Pattern must be programmed. This output activates according to the bell pattern and remains active until the bell time expires or is manually silenced.
Silent Bell must be set to No in order for the bell to ring upon alarm.
Each area can be assigned a unique output number for each of the events listed in this section.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to a value other than **0** for each enabled area. See SIA CP-01 Verification for more information.
Reference
Output Parameters > Area Wide Outputs > Alarm Bell

Fire Bell

Default: A
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when a fire point assigned to this area goes into alarm. Fire Time and Fire Patern must be programmed in Bell Parameters. This output activates according to the Bell Pattern and remains active until the bell time expires or is manually silenced. It will also activate for keypad fire alarms.
Each area can be assigned a unique output number for each of the events listed in this section.
IMPORTANT: To meet UL864 requirements, set this parameter to a value other than **0**.
Reference
Output Parameters > Area Wide Outputs > Fire Bell

Reset Sensors

Default: C
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
Unlike the default output for Alarm Bell and Fire Bell, this voltage output (output C) output de-activates for five seconds when the RESET SENSORS? function is initiated from the keypad or during a FIRE WALK? test.
The Reset Sensor time converts from the five second default time to the time programmed in Restart Time (Area parameters section) when a point programmed for Alarm Verify (Point Index Section) goes into an alarm condition.
When sharing one output to reset sensors in two or more areas you must program the following. Failure to do so can cause TROUBLE PT ### for all point types programmed as Resettable:
– Scope must include all the areas that are sharing the output.
– Reset Sensors for the user initiating the sensor reset must be enabled in all the areas that are sharing the output.
– Restart Time must be the same number of seconds for all the areas that are sharing the output.
Each area can be assigned a unique output number for each of the events listed in this section.
IMPORTANT: To meet UL864 9th edition requirements, set this parameter to a value other than **0**.
Reference
Output Parameters > Area Wide Outputs > Reset Sensorrs

Fail To Close/Part On Armed

Default: 0
Selections:
– D9412GV4: **Blank, 0 to 128, A, B or C**
– D7412GV4: **Blank, 0 to 64, A, B or C**
NOTE: To change between the **Fail To Close** and **Part On Armed** output functions described below, configure the **Miscellaneous >> Part On Output** parameter.

This output activates when the closing window expires for the specified area. It remains activated until midnight, or until another closing window starts, or the panel is reset, whichever occurs first.
Each area can be assigned a unique output number for each of the events listed in this section.
This output activates when all areas assigned to the same output are armed Part On Instant or Part On Delayed.
RPS Menu Location
Output Parameters > Area Wide Outputs > Fail to Close/Part On Armed

Force Armed

Default: 0
Selections:
– D9412GV4: Blank, 0 to 128, A, B or C
– D7412GV4: Blank, 0 to 64, A, B or C
This output activates when this area is force armed. It remains activated until the area is disarmed or the control panel is reset.
This output does not activate when Part On force arming.
Each area can be assigned a unique output number for each of the events listed in this section.
RPS Menu Location
Output Parameters > Area Wide Outputs > Force Armed

Watch Mode

Default: 0
Selections:
– D9412GV4: Blank, 0 to 128, A, B or C
– D7412GV4: Blank, 0 to 64, A, B or C
This output activates when a controlled point programmed for Watch Point is tripped in the specified area while the area is in Watch Mode and the point is not armed. It remains activated for two seconds after each point is faulted.
Each area can be assigned a unique output number for each of the events listed in this section.
Reference
Output Parameters > Area Wide Outputs > Watch Mode

Area Armed

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
The output activates when the specified area becomes All On (exit delay must expire before the output activates). The output remains activated until the area is disarmed, it does not deactivate during the entry delay time.
If multiple areas use the same output, the output activates when all areas are armed. It deactivates when the first area disarms.
– Keyswitch area armed status with LED's. Use an output module and connect an LED to display the armed state.

– Alternate communication trigger: This output can be used to trigger the input zone of a device being used as a slave to report panel arming status.

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

Reference

Output Parameters > Area Wide Outputs > Area Armed

Area Off

Default: 0

Selections: A, B, C, 0-64

When an area's arming state switches from All On (either delay or instant) to Part On or Disarmed, the output number configured here activates.

When an area's arming state switches from Part On or Disarmed to All On (either delay or instant), the output number configured here de-activates.

If the same output number is configured in more than one area's Area Off Output, the output will only activate when the first area is no longer armed All On. If the same output number is configured in more than one area's Area Off Output, the output will only de-activate if all area's using that same output number are armed All On.

The Area Off Output is also affected by the Early Area Armed Output. When Early Area Armed Output is set to **No**, the Area Off Output does not activate until the end of exit delay. When the Early Area Armed Output is set to **Yes**, the Area Off Output de-activates as soon as exit delay starts and the area is armed All On.

Note: if the All On - No Exit option is set to Yes and the area switches to Part On at the end of exit delay, the Area Off Output will activate at that time.

Simply starting entry delay does not affect the state of the output configured in Area Off.

RPS Menu Location

Output Parameters > Area Wide Outputs > Area Off

Area Fault

Default: 0

Selections:

– D9412GV4: Blank, 0 to 128, A, B or C
– D7412GV4: Blank, 0 to 64, A, B or C

The output activates whenever a Part On, Interior or Interior Follower point is faulted. The output remains activated until all perimeter and interior points in the area are normal.

Keyswitch area fault status with LED's: Use an output module and connect an LED to illuminate when this output is activated indicating that the area is not ready to arm. Assign a unique output number for each area.

RPS Menu Location

Output Parameters > Area Wide Outputs > Area Fault

Duress Output

Default: 0

Selections:

– D9412GV4: Blank, 0 to 128, A, B or C
– D7412GV4: Blank, 0 to 64, A, B or C

The output activates when a duress alarm is generated from a keypad assigned to the specified area.
Burg Time must have a bell period programmed and Duress Enable must be set to Yes. This output activates "steady" regardless of bell pattern and remains active until the bell time expires.
Each area can be assigned a unique output number for each of the events listed in this section.

Reference

Output Parameters > Area Wide Outputs > Duress Output

Part On Fault

Default: 0

Selections:

- D9412GV4: Blank, 0 to 128, A, B or C
- D7412GV4: Blank, 0 to 64, A, B or C

The output activates when a controlled Part On point assigned to the specified area is faulted. This output activates regardless of the areas armed state. This output provides a steady output until all perimeter points in the area return to normal.
This output does not activate on interior faults. To detect all area point faults, program all points as Part On points in the area to which this output is assigned.
Assign a unique output number for each area.

RPS Menu Location

Output Parameters > Area Wide Outputs > Part On Fault

Silent Alarm

Default: 0

Selections:

- D9412GV4: Blank, 0 to 128, A, B, or C
- D7412GV4: Blank, 0 to 64, A, B, or C

This output activates when a point assigned to the specified area and programmed for Silent Bell goes into alarm.
Use this output for invisible/silent bell 24-hour panic/hold up applications.

IMPORTANT: To meet UL864 requirements, set this parameter to a value other than **Blank**.

Reference

Output Parameters > Area Wide Outputs > Silent Arm

Gas Bell

Default: A

Selections: 0, 1 to 255, A, B or C

This output activates when a gas point assigned to this area goes into alarm.
The area-wide Gas alarm bell uses the time in Fire Bell Time and output cadence defined in Gas Pattern. This output activates according to the bell pattern and remains active until the bell time expires or is manually silenced.
Each area can be assigned a unique output number for each of the events listed in this section.

RPS Menu Location

Output Parameters > Area Wide Outputs > Gas Bell

9.2 Panel Wide Outputs

AC Failure

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when the control panel responds to an AC power failure as programmed in AC Fail Time. This output automatically resets when AC power is restored.
Connect a separate sounder to this output to create an audible annunciation from the keypads for all applications excluding commercial fire systems.
Reference
Output Parameters > Panel Wide Outputs > AC Failure

Battery Trouble

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output 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 output automatically resets when battery power is restored.
Connect a separate sounder to this output to create an audible annunciation from the keypads for all applications excluding commercial fire systems.
Reference
Output Parameters > Panel Wide Outputs > Battery Trouble

Phone Fail

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when a telephone line failure alarm is generated. A time must be entered in Phone Supervision Time in order for this output to activate.
This output automatically resets when a valid passcode is entered at the keypad.
Reference
Output Parameters > Panel Wide Outputs > Phone Fail

Comm Fail

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when the control panel is unable to send a report after 10 attempts are made to each routing destination. At the same time, COMM FAIL RT ## displays on the keypad.

This output automatically resets when a report is sent successfully.
Use this output to report primary digital report failure to an alternate communication device.

Reference

Output Parameters > Panel Wide Outputs > Comm Fail

Log % Full

Default: 0

Selections:

- D9412GV4: 0 to 128, A, B or C
- D7412GV4: 0 to 64, A, B or C

Enter the number of the output that activates when the log has reached the programmed percentage of its capacity as programmed in Log % Full.
This output provides a steady output until the RPS pointer is set. See Get History for more information.

Reference

Output Parameters > Panel Wide Outputs > Log % Full

Summary Fire

Default: 0

Selections:

- D9412GV4: 0 to 128, A, B or C
- D7412GV4: 0 to 64, A, B or C

Enter the number of the output that activates when any fire point in the system (Type 0 and Fire both are set to Yes) goes into alarm.
This output provides a steady output until all fire points in the system are returned to normal, and all fire alarm events are cleared from keypad displays.

IMPORTANT: This parameter only functions as described when Fire Summary Sustain (**Miscellaneous > Fire Summary Sustain**) = **No**.

Reference

Output Parameters > Panel Wide Outputs > Summary Fire

Summary Alarm

Default: 0

Selections:

- D9412GV4: 0 to 128, A, B or C
- D7412GV4: 0 to 64, A, B or C

Enter the number of the output that activates when a non-fire point goes into alarm.
A steady output is provided until the alarm is silenced and the alarm event is cleared form the keypads' display .
This output does not activate for silent alarms.

Reference

Output Parameters > Panel Wide Outputs > Summary Alarm

Summary Fire Trouble

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when any fire point on the control panel is in trouble. This output provides a steady output until all fire points have restored to a normal condition.
Reference
Output Parameters > Panel Wide Outputs > Summary Fire Trouble

Summary Supervisory Fire

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when any fire supervisory point on the control panel is in a supervisory condition (off normal).
This output provides a steady output until all fire supervisory points are restored to a normal condition.
Reference
Output Parameters > Panel Wide Outputs > Summary Supervisory Fire

Summary Trouble

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when any non-fire/gas point on the control panel is in a trouble condition. A steady output until the trouble is provided until the event message is cleared by the user at the keypad.
Note: Fire/gas trouble points must be restored to normal before summary outputs can be cleared.
Reference
Output Parameters > Panel Wide Outputs > Summary Trouble

Summary Supervisory Burg

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This output activates when any non-fire/gas supervisory point on the control panel is in a supervisory condition. A steady output is provided until the event message is cleared by the user at the keypad.
Note: Fire/gas supervisory points must be restored to normal before summary outputs can be cleared.
Reference
Output Parameters > Panel Wide Outputs > Summary Supervisory Burg

Summary Gas Output

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This parameter sets the number of the output that activates when any gas point in the system goes into alarm.
A steady output is provided until all gas points in the system are returned to normal.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Summary Gas Output

Summary Gas Supervisory Output

Default: 0
Selections:
– **D9412GV4:** 0 to 128, A, B or C
– **D7412GV4**: 0 to 64, A, B or C
This parameter enables the output to activate when any gas supervisory point on the control panel is in a supervisory condition (off normal). A steady output is provided until all gas supervisory points are restored to a normal condition.
Reference
Output Parameters > Panel Wide Outputs > Summary Gas Supervisory Output

Summary Gas Trouble Output

Default: 0
Selections:
– D9412GV4: 0 to 128, A, B or C
– D7412GV4: 0 to 64, A, B or C
This parameter sets the output to activate when any gas point on the control panel is in trouble. A steady output is provided until all gas points have restored to a normal condition.
0 Disable
1-128 Point number
A Onboard Output A
B Onboard Output B
C Onboard Output C
Reference
Output Parameters > Panel Wide Outputs > Summary Gas Trouble Output

9.3 Output Configuration

Output source

Default:
– Output A, B, C On-Board,
– All others Zonex
Selections: On-Board, Zonex, Octo-output
On-Board Output A, B and C are on-board outputs. This is a reference only selection.
Zonex The output is installed on a Zonex bus output module.

Octo-input The output is installed on an SDI2 bus input module. This would indicate that a B308 is being used.
The Output Destination field provides two benefits when configuring outputs on a GV4 Series Control Panel.
First, the Output Destination field guides the RPS operator with configuration rules, where the B308 Octo-output devices are allowed to be configured, and what outputs ranges are permitted. When a selection is grayed out or unavailable as a selection, that option is not allowed when configuring that particular Output number.
Second, the Output Destination field gives a description for the physical location of the point for use by installation and service personnel.

IMPORTANT: A B308 Octo-output module can be installed on particular Output number boundaries starting at Output 11. Refer to B308 Octo-output Switch Settings.

Reference
Output Parameters > Output Configuration > Output Destination

Output Descriptions

Default:
- D9412GV4:
- **Output A:** OUTPUT A
- **Output B:** OUTPUT B
- **Output C:** OUTPUT C
- **Outputs 1 to 128:** Blank
- D7412GV4:
- **Output A:** OUTPUT A
- **Output B:** OUTPUT B
- **Output C:** OUTPUT C
- **Outputs 1 to 64:** Blank

Selections: Up to 24 alphanumeric characters
Enter up to 24 characters of text to describe the output.
This is for informational purposes only and is not sent to the control panel.

Reference
Output Parameters > Output Configuration > Output Descriptions

10 Passcodes

10.1 Passcodes & Authority Levels

User Name (Passcodes)

Default:
- User 0: Installer
- Users 1 to 999 (D9412GV4 only): USER 1 - USER 999
- Users 1 to 399 (D7412GV4 only): USER 1 - USER 399

Selections: 16 alphanumeric characters (enter using capital letters)
Invalid Characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), brackets ([]), forward slash (\), vertical bar (|), and colon (:).
Enter up to 16 characters of text for this user group.
Programming this group with a departmental, team or function name identifies all the users in this group in a function-related manner (for example, ENGINEERING).
IMPORTANT: User 0 applies only to passcodes and authority levels. There is no User 0 for access site codes and card data.

Reference
Passcodes > Passcodes & Authority Levels > User Name

Passcode

Default:
- D9412GV4:
- User 0: 123
- User 1: 123456
- Users 2-999: Blank
- D7412GV4:
- User 0: 123
- User 1: 123456
- Users 2-399: Blank

Selections: Enter a 3-to-6-digits based on the entry made in Passcode Length.
IMPORTANT:
- User 000 is the Service Authority Level (Level 15). You cannot change the programming for User 000. Only the Service Authority Level (User 000) can delete User 000. When a user other than User 000 tries to delete the passcode for User 000, the keypad displays NOT IN USE. User 000 cannot be added or changed at the keypad.
- To meet UL864 requirements, enter at least one passcode when installing a commercial fire alarm system.

Enter a value from three to six digits in length to enable a passcode for the Master User in this group.
You cannot enter any passcode number that could conflict with a duress passcode. Regardless of the Duress Type setting, passcodes within a range of 2 for existing passcodes cannot be entered. This rule applies even if duress is disabled. For example, once a passcode of 654327 is entered, 654325, 654326, 654328, and 654329 cannot be entered.

A silence bell authority is built into all authority levels, even if they are default and none of the available programmable functions are enabled. A user passcode can silence a Fire/Burg bell as long as any authority level is assigned to the area where the bell can be silenced from.

Reference

Passcodes > Passcodes & Authority Levels > Passcode

User Group

Default: 0

Selections: 0 to 8

Use this parameter to create a group of up to 999 users for the D9412GV4 (399 users for the D7412GV4), whose combinations can be enabled/disabled using an automatic user window. This is the number that is entered into the *User Group* (Schedules > User Group Windows) for any active 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 8:00 AM and 4:00 PM. Between 4:00 PM and 8:00 AM the next day, the users cannot use their passcodes.

To enable this user's passcode at all times, leave this item blank.

IMPORTANT: User Group Window times cannot be changed from the keypad. Once 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 RPS.

Reference

Passcodes > Passcodes & Authority Levels > User Group

Area# Authority

Default:

- User 0: 15 (A1 to A32 Authority)
- User 1:
- D9412GV4: A1 Authority = 1, A2 to A32 Authority = 0
- D7412GV4: A1 Authority = 1, A2 to A8 Authority = 0
- Users 2 to 999 (D9412GV4 only): 0 (A1 to A32 Authority)
- Users 2 to 399:
- D7412GV4: 0 (A1 to A8 Authority)

Selections: 0 (No Authority), 1 to 14

Assign an authority level to the user for this area.

0 (zero) means the user has no authority in this area.

IMPORTANT:

- The D9412GV4 supports up to 32 areas, the D7412GV4 support up to 8 areas.
- To meet UL864 requirements, assign a valid authority level to the passcode used to silence bells.

Reference

Passcodes > Passcodes & Authority Levels > Area# Authority

10.2 Access Site Codes & Card Data

User Name

Default for User Name (Within Passcodes>Passcodes & Authority Levels):
- Users 0 to 999 (D9412GV4 only): SERVICE PASSCODE, USER 1 - USER 999
- Users 0 to 399 (D7412GV4 only): SERVICE PASSCODE, USER 1 - USER 399

Selections: 32 alphanumeric characters

Default for User Name (Within Passcodes >Access Site Codes & Card Data):
- Users 1 to 999 (D9412GV4 only): USER 1 - USER 999
- Users 1 to 399 (D7412GV4 only): USER 1 - USER 399

Selections: 32 alphanumeric characters
This parameter sets what is displayed at keypads.
Enter up to 32 characters of text to identify the user group.
- SDI2 keypads display the first 20 characters. If more than 20 characters are used, the text scrolls across the display one time. To scroll the text again, press [ESC].
- Spaces before, after and within a string of text are treated as text and are included in the 32 character limit.
- On SDI keypads, only the first 16 characters display.

Programming this group with a departmental, team or function name identifies all the users in this group in a function-related manner (for example, ENGINEERING).
RPS Menu Location
Passcodes > Access Site Codes & Card Data > User Name

Site Code

Default (for the following card types):
26 bit: 255
37 bit: 0
Selections:
26 bit: 0 to 255 (255 = disabled). Enter the site code, as indicated on the packaging of the tokens or cards. The site code can also be derived by learning the token or card into the system (MENU 42), then receiving the control panel programming with RPS. To delete a card, enter the default number for that card type in this parameter.
37 bit: 0 is the only valid value for this card type. To delete a card, delete the value and leave the field blank.
IMPORTANT: Always pre-tag your tokens prior to adding them to the system so you do not mix them up. Use the CRD ID ###-# number to index them.
Reference
Passcodes > Access Site Codes & Card Data > Site Code

Card Data

Default: Blank
Selections:
26 bit card type: 0 to 65534, or Blank
37 bit card type: 0 to 4294967294, or Blank

26 bit: You must program the appropriate Site Code parameter before programming this parameter. Enter the five remaining decimal numbers on the back of the token/card.
37 bit: Enter the decimal numbers on the back of the token/card (up to ten decimal numbers).
Reference
Passcodes > Access Site Codes & Card Data > Card Data

RFID (B820 Inovonics Wireless)

Default: 0
Selections: 0 - 99999999
Each user can be assigned a wireless keyfob RFID (Radio Frequency device Identification number). 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 user's Keyfob. An RFID 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.
IMPORTANT:
- Duplicate ID detection must be based on the RFID value stored in configuration memory, not on the number printed on the device.
- Keyfobs are not supervised when assigned to a user.

Reference
Passcodes > Access Site Codes & Card Data > RFID (B820 Inovonics Wireless)

RFID (B810 RADION Wireless)

Default: 0
Selections: 11 - 167772156
Each user can be assigned a wireless keyfob RFID (Radio Frequency device Identification number). 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 user's Keyfob. An RFID 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.
IMPORTANT:
- Duplicate ID detection must be based on the RFID value stored in configuration memory, not on the number printed on the device.

Reference
Passcodes > Access Site Codes & Card Data > RFID (B810 RADION Wireless)

Supervised

Default: No
Selections: Yes/No
This parameter supervises the presence of keyfobs assigned to the area.
Yes Keyfobs are reported as missing when removed from an assigned area.
No Keyfobs are not reported as missing when removed from an assigned area.
This parameter can be set individually for each key fob. When enabled, the keyfob is supervised in four-hour intervals.
Reference
Passcodes > Access Site Codes & Card Data > Supervised

11 Points

11.1 Point Indexes

Index Description

Default:
- **Point Index 1:** 24-hr Instant Open/Short
- **Point Index 2:** 24-hr Inv/Sil on Short
- **Point Index 3:** Pull Station
- **Point Index 4:** Smoke Detector
- **Point Index 5:** Smoke Det w/Verification
- **Point Index 6:** Bell Supervision
- **Point Index 7:** Part On: Instant
- **Point Index 8:** Part On: Delay
- **Point Index 9:** Prt: Inst Local:Dis
- **Point Index 10:** Interior: Instant
- **Point Index 11:** Interior: Delay
- **Point Index 12:** Int: Inst Local:Dis
- **Point Index 13:** Interior: Follower
- **Point Index 14:** Maintained Keyswitch
- **Point Index 15:** Momentary Keyswitch
- **Point Index 16:** Open/Close on Fault
- **Point Index 17:** Gas
- **Point Index 18:** Gas: Supervisory
- **Point Index 19:** Aux AC Supervision
- **Point Index 20:** Part On: Watch Off
- **Point Index 21:** Part On: POPIT Motion
- **Point Index 22:** Fire Supervisory on Open
- **Point Index 23:** Non-Fire Supervisory Op
- **Point Index 24:** Local: Buzz on Fault
- **Point Index 25:** Prt: Delay
- **Point Index 26:** Part On: Instant
- **Point Index 27:** Part On: Delay
- **Point Index 28:** Interior: Follower
- **Point Index 29:** Interior: Instant
- **Point Index 30:** Interior: Delay
- **Point Index 31:** 24-hr Instant Open/Short

Selections: Up to 24 alphanumeric characters

Enter up to 24 characters of text to describe the point index.

This is for informational purposes only and is not programmed in the control panel.

RPS Menu Location

Points > Point Indexes > Index Descriptions

Point Type

Default: (Reference Index Descriptions below)

- Point Indexes 1, 2, 6, 23, 31: ..... 24 Hour
- Point Indexes 3 to 5, 22: ..... Fire Point
- Point Indexes 7 to 9, 20, 21, 24-27: ..... Part On
- Point Indexes 10 to 12, 29, 30: .... Interior
- Point Index 13, 28: ..... Interior Follower
- Point Index 14: ..... Keyswitch Maintained
- Point Index 15: ..... Keyswitch Momentary
- Point Index 16: ..... Open/Close Point
- Point Index 17, 18: ..... Gas Point
- Point Index 19: ..... AUX AC Supervision

Selections: 0 to 6, 10-12

This entry defines the point type.

 # -- Index Description

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 panic, medical, and police alerts.

24-hour points can be programmed as bypassable. However, the application should be carefully considered before using the bypassable option. Bypassable 24-hour points should be programmed to Buzz on Fault.

When a 24-hour point is bypassed, the report should be sent as it occurs. If the area contains all 24-hour points, the area is never armed or disarmed; therefore, a deferred bypass report is not sent.

24-hour protection for fire doors, roof hatches, etc. Instead of programming this type of protection as a 24-hour point, consider using a Part On point type with a Point Response of 9 to E. 24-hour points do not show faults when an arming function is entered, but Part On points do. When programming for this type of protection, you should consider using the Buzz On Fault and Local While Disarmed options.

Part On

Part On points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using Part Oning functions) separately from points programmed as interior. This lets the user partially arm the system to establish perimeter protection and still occupy the interior of the protected premises.

Part On points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.

When a Part On point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Part On point trips, the panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Part On point's entry delay time is less than the remaining time, it shortens the entry delay time.

Part On points programmed for an instant Point Response , generate an alarm immediately when tripped, even during entry or exit delay.

Interior

Interior points are armed only by arming All On the area. They are not armed when using Part Oning functions. These points are typically used to monitor interior detection devices such as interior doors, motion detectors, photoelectric beams, and carpet mats.

Interior points can be either Instant or Delayed:

- **Instant:** Interior points are usually programmed for an instant alarm (see Point Response). Points programmed for instant alarms generate alarms immediately, even during entry or exit delay.
- **Delayed:** Interior Points can be programmed for a delayed Point Response . A delayed response means that if the point is tripped while the area is armed, it initiates entry delay. It does not generate an alarm until entry delay expires.

When an interior point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when the interior point trips, 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.

Delayed points can also initiate an entry tone at the keypad (see Entry Tone Off).

IMPORTANT: In some cases, you might need to create an interior point that causes an instant alarm only if entry delay protection is not tripped first. Use Interior Follower to create this type of protection.

Interior Follower

Interior follower points are armed only by all on arming the area. They are not armed when using Part Oning functions.

An interior follower point does not create an alarm if it trips while the area is in entry delay. An interior follower does not change the amount of remaining entry delay time. If no entry delay is in effect when the interior follower trips, it creates an instant alarm.

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 Entry Delay for an interior follower point.

IMPORTANT: It might be necessary to increase the Debounce count for interior follower points to prevent interior follower points from going into alarm before the control panel recognizes that a Part On delay point has been faulted. Program the interior follower point's Debounce for one number higher than the debounce count on Part On delay points.

Keyswitch Maintained

Program Point Response as 1. Do not connect initiating devices to a keyswitch point.

- Normal: The area is disarmed.
- Open: When this point changes from normal to open, the area arms.
- 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.

If you program Point Response as 2, the point responds as follows:

- Normal: When this point changes from open to normal, the area arms.
- Open: The area is disarmed.
- 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.

Trouble and restoral reports are not sent if Local Disarmed is set to Yes.

Alarm and restoral reports are not sent if Local Armed is set to Yes.

IMPORTANT: Point Response 2 is required for Inovonics FA113 Wireless Keyfobs.

Keyswitch Momentary

Used for area arming and disarming. Point Response must be programmed 1. Do not connect initiating devices to a keyswitch point.

- N–>S–>N: When this point momentarily changes from normal to shorted to normal, it toggles the armed state of the area.
- 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.

Trouble and restoral reports are not sent if Local Disarmed is set to Yes.
Trouble and restoral reports are not sent if Local Armed is set to Yes.

Open/Close Point

Used for point arming and disarming. Point Response must be programmed 1. Local bells are silenced through the keypad.

- Normal: The point is armed and sends a `POINT CLOSING`. `Point Closing` is not sent if Local Armed is set to Yes.
- Open: An open is an alarm while the point is armed. An open is a trouble while the point is disarmed. `ALARM` and `RESTORAL` reports are not sent if Local Disarmed is set to Yes.
- Short: The point is disarmed and sends a `POINT OPENING`. A `Point OPening` is not sent if Local Armed is set to Yes.

Fire Point

This point type generates a Fire Alarm when the instant alarm response is activated (Refer to 24-hour point response section). Fire Alarms are the highest priority event in the control panel. Refer to Fire Point Characteristics section for further details.

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. This point type does not use Point Response; therefore, no alarm condition occurs.
If this point type is bypassed, **24 HOUR PT BYPASSED** is shown on the keypads.

Gas Point

This point type monitors gas detection sensors and generates Gas Alarm when instant alarm response is activated (Refer to 24-hour point response section).

Custom Function

This point type activates a Custom Function when the CF point response is activated (Refer to the Custom Function Point response table). The Custom Function activated is configured in Custom Function parameter.
Custom Function points do not support the following features:

- Buzz on Fault
- Watch Point, Output Response Type
- Display as Device
- Cross Point, Invisible Point
- Silent Bell
- Local While Disarmed
- Local While Armed.

Reference

Points > Point Indexes > Point Type

Point Responses — Overview

Applications for Point Responses 9, D, and E

You can combine Point Responses 9, D and E with perimeter Point Types to create more flexible 24-hour protection. Unlike 24-hour points, a faulted Part On 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 for Zonex/Asic motion detectors. This allows troubles to report while the panel is All Oned.
Point Response F will not sound local Keypads but will activate Output Response Type and keypad faults. To annunciate the off-normal state at a keypad, set Display as Device to Yes, and/or Buzz On Fault as 1 or 2. This point response does not generate alarms or activate alarm output.
Point Response 8, 9, A, B, and C provide supervisory (24 hour) reporting.

Fire Point Characteristics

- Reporting: Fire reports are the first events that the control panel sends when a group of events occur.
- Visual Annunciation: Fire Troubles continue to scroll until the trouble is cleared. Once acknowledged, a FIRE TROUBLE scroll lets the end user know that a fire point, or group of Fire points, is still in trouble. Panel Wide Outputs Summary Fire and Summary Fire Trouble activate if a output is assigned when any fire point goes into alarm or is in trouble.
- Audible Annunciation: A Fire point activates the Fire Bell. The amount of time and pattern of the output activation is programmed by area in Fire Time and Fire Pattern.
- Supervisory: A Fire point can send a `FIRE SUPERVISORY` report and activate the Summary Supervisory Fire and Summary Fire Trouble panel wide outputs with a Point Response of 8-9-A-B-C.
- Alarm Verification: A Fire point can delay an alarm by the time programmed in Restart Time in the Area parameters. Combined with Resettable, a fire point also resets the electrical circuit for the amount of restart time.
- Reset Sensor: A fire device that requires resetting can be manually reset using the reset sensor output for the area it is assigned to.
- Fire Walk: Use the Fire Walk function to test fire points in the system.

To provide an audible tone for a Fire Supervisory point that has been restored, use Output Response Type and connect to a graphic annunciator.
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 (D1256 and D1257).

Point Response

Default: (Reference the tables below for a description of the response value)

- Point Index 1: 0
- Point Indexes 2-5: 1
- Point Index 6: 9
- Point Index 7: 0
- Point Index 8: 8
- Point Index 9: 9
- Point Index 10: 0
- Point Index 11: 8
- Point Index 12: 9
- Point Index 13: 8
- Point Indexes 14-16: 1

- Point Index 17: 1
- Point Index 18: 9
- Point Index 19: 1
- Point Index 20: 0
- Point Index 21: E
- Point Indexes 22-23: 8
- Point Index 24: F
- Point Index 25: 8
- Point Index 26: 0
- Point Indexes 27-28: 4
- Point Index 29: 0
- Point Index 30: 4
- Point Index 31: 0

Selections: 0 - 9, A - F

Point Response defines the "Point Response to Opens and Shorts" for this point. The Point Response tables show each selection available for controlled (non-24-Hour) point types and 24-Hour point types.

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		

Key: I = Instant Alarm D = Delayed Alarm T = Trouble S = Supervisory Blank = Audible/visual response

Example: Point Type = 1 and Point Response = 8. Part On point with delayed alarm response when armed (opened or shorted) and no response when disarmed.

24-Hour Points

Point Response	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Open	I	T	I	T			I	T	S	T	S		S			
Short	I	I	T	T	I	T			T	S		S	S			

Key: I = Instant Alarm D = Delayed Alarm T = Trouble S = Supervisory Blank = Audible/visual response

Example: Point Type = 0 and Point Response = 8. 24-hour point with supervisory response when open and a trouble response when shorted.

Custom Function Point Response																
Point Response		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Short						CF		CF	CF	T	CF		CF	CF	T	
Armed	Open							CF	CF	T	CF		CF	CF	T	CF	
Disarmed	Short	CF		CF	CF	T	CF		CF	CF	T						
Disarmed	Open		CF	CF	T	CF		CF	CF	T	CF						
Key: CF = Execute Custom Function T = Trouble Blank = no response																	

When programming the Point Response for Inovonics Wireless Transmitters, remember that regardless of how the transmitter is programmed (Normally Open vs. Normally Closed), the Wireless Interface always sends the off-normal state to the control panel as a short and a tamper condition as an open. As a result, typical Point Responses for the Inovonics transmitters would include 0, 1, 6, 7, and E for Controlled points and 0 and 1 for 24-hour burg points. When programming a transmitter as a fire point, a Point Response of 1 is recommended.

IMPORTANT: Wireless transmitters are not UL Listed with the D9412GV4 or D7412GV4 control panels in fire or burglary applications.

RPS Menu Location

Points > Point Indexes > Point Response

Entry Delay

Default: 30 seconds

Selections: 5 - 600 seconds (5-second increments)

Use this option to enter the amount of entry delay time that a user has after faulting a controlled point *(Part On, Interior or Interior Follower*) with a delayed response (D) (Point Response) of 4, 5, 6, 7, or 8.

On the keypad's display, `DISARM NOW` appears for the duration of the time programmed when the point is faulted in the delay condition. The keypad display alternates between `DISARM NOW` and the point text of the point that caused the area to enter into Entry Delay.

If this time is allowed to expire before disarming or if the point is faulted to an instant response (I) an alarm occurs.

Make entries in five-second increments. The programmer does not allow off-increment entries.

Passcode Disarm activates when the last digit of the passcode is pressed. The [ENTER] key is allowed, but not required, when entering a passcode during Entry Delay.

If a subsequent 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 Part On point is faulted and Entry Delay starts. If an interior point must fault during Entry Delay to allow the user to disarm the area at a keypad, program Point Type as Interior Follower.

IMPORTANT:
- To comply with UL standards, the total amount of time entered in Entry Delay and Alarm Event Abort must not exceed 1 minute.
- To comply with SIA CP-01 False Alarm Reduction, set this parameter between 30 and 240 seconds for all point indexes. See SIA CP-01 Verification for more information.

RPS Menu Location
Points > Point Indexes > Entry Delay

Entry Tone Off

Default: No (for all Point Indexes)
Selections: Yes/No
This option enables/disables the entry delay warning tone for this point.
Entry Tone can also be turned off when programming your Entry Tone in the keypad section which allows you to manage the tone by keypad.
You might want to disable the entry tone in high security applications where you do not want to annunciate entry delay.
Yes: Disable entry delay tone when this point is faulted to the delay response.
No: A tone sounds at keypads when this point initiates entry delay.
CAUTION: Do not set this parameter to No on points used to notify the user to disarm the system. The possibility of false alarms increases if the entry delay warning is not used.
Reference
Points > Point Indexes > Entry Tone Off

Silent Bell

Default:
- Point Index 1: No
- Point Index 2: Yes
- Point Indexes 3 to 31: No

Selections: Yes/No
This parameter determines whether the bell and keypad sounders activate upon an alarm event for non-fire/gas points. Fire and Gas points ignore this parameter setting and always activate the bell and sound the alarm tone at keypads when this point goes into alarm.
If you want this point to eventually ring the bell because the message failed to reach the central station receiver, set Audible After 2 Failures to Yes.
IMPORTANT: To meet UL864 requirements, set this parameter to **No**.
Yes: Activate the Silent Alarm output when this point goes into alarm. Do not activate the Alarm Bell output or keypad alarm sounders. This setting only applies to non-fire/gas points.
No: Activate the Fire Bell, Gas Bell or Alarm Bell output and sound the alarm tone at Keypads when this point goes into alarm. If this is a fire point, it activates the Fire Bell. If this point is a gas point, it activates the Gas Bell, otherwise, it activates the Alarm Bell. The amount of time and pattern of the output activation is programmed by area.
Reference
Points > Point Indexes > Silent Bell

Ring Until Restored

Default: No (for all Point Indexes)
Selections: Yes/No
Use this parameter for fire or gas applications to meet the requirement that audible alarms cannot be silenced until the fault condition clears.
IMPORTANT: If the point restores and the originating alarm is not silenced from the keypad, the alarm output continues until Fire Bell or Gas Bell time expires. If the point does not restore, the alarm output continues even after bell time expires.
Yes: Fire or Gas Bell output and keypad sounders for this point cannot be deactivated, from a keypad or upon bell timeout, until the point is restored to normal.
No: Fire or Gas Bell output and keypad sounders for this point can be deactivated, either from a keypad or upon bell timeout, whether or not the point has been restored to normal.
Reference
Points > Point Indexes > Ring Until Restored

Audible After 2 Fails

Default: No (for all Point Indexes)
Selections: Yes/No
Yes: For silent points, Alarm Bell output activates after two failed attempts to send the report to the central station.
No: Silent Bell points do not cause the Alarm Bell output 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 alarm bell. A silent alarm is generated when a point with Silent Bell set to Yes is alarmed.
When a point programmed for Silent Bell is faulted, Burg Time starts even though the bell is not yet ringing. It could take up to three minutes before the second attempt has failed. Because of this, ensure Burg Time is set to provide the amount of bell time you would like, minus the three minutes it might take before the bell actually begins to ring.
Reference
Points > Point Indexes > Audible After 2 Fails

Invisible Point

Default:
- Point Index 1: No
- Point Index 2: Yes
- Point Indexes 3 to 31: No

Selections: Yes/No
Use this option to determine whether the point appears in the keypad display upon an alarm condition. Point text appears and annunciation is made for invisible points that are programmed for a trouble condition in point response.
To prevent the keypad alarm tone and the Alarm Bell from sounding, this point must have Silent Bell set to Yes.
ALARM SILENCED displays at the keypad if this invisible point causes a bell to ring upon an alarm and a valid passcode is entered.
Note: Fire and Gas points always function as if this parameter is set to No.

IMPORTANT: To meet UL864 requirements, set this parameter to **No**.

Yes: Keypads do not display alarm activity from this point.

No: Activity from this point is visible at the keypads.

RPS Menu Location

Points > Point Indexes > Invisible Point

11.1.1 Buzz On Fault

Default:

- Point Indexes 1-8: 0
- Point Index 9: 1
- Point Indexes 10 to 31: 0

Selections: 0 to 3

Use this option to generate a Trouble Buzz even if the point is not actually in trouble. This does not affect normal point trouble (T) buzz.

The buzz does not automatically stop once the point is restored when using Selections 1 or 2. The user must acknowledge the buzz prior to the buzz stopping. However, when using Selection 3, the trouble tone stops when the point restores to normal.

If the fault occurred while the system was armed or if it was a 24-hour point and in both cases an alarm occurred, the buzz follows the silencing of the bell or at the end of the bell time.

Refer to the following table for Buzz on Fault controlled point operation and 24-hour point operation:

Selection	Operation for Controlled Points (Part On, Interior or Interior Follower)	Operation for Non-Controlled Points (24-Hour)
0	The point buzzes at the keypad only if it enters into the trouble condition indicated in Point Response.	Same operation as 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 ENTER key. 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 ENTER key. 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	The point buzzes at the keypad for any fault condition regardless of the armed state. The user cannot silence this buzz, but it

	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.	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.

Reference
Points > Point Indexes > Buzz On Fault

Watch Point

Default:
- Point Indexes 1 to 6: No
- Point Indexes 7 to 8: Yes
- Point Indexes 9 to 25: No
- Point Indexes 26 to 27: Yes
- Point Indexes 28 to 31: No

Selections: Yes/No
Use this option to allow a controlled point to generate a watch tone as long as the area is disarmed and not being faulted into a trouble or alarm condition.
Yes: This point activates Watch Mode responses if it is faulted when the control panel is in Watch Mode.
No: Do not activate Watch Mode responses for this point.
Reference
Points > Point Indexes > Watch Point

Output Response Type

Default:
- Point Indexes 1 to 23: 0
- **Point Index 24:** 1
- **Point Indexes 25 to 31:** 0

Selections: 0, 1, 2

0 Point state does not affect the operation of the corresponding output.

1 Output Follow Point: The output corresponding with this point activates when the point is faulted to any off normal state, even if the point is bypassed. The output automatically resets when the point is returned to normal.

2 Output Latches: The output corresponding with this point latches when the point goes into an alarm condition. This output remains on steady output until the alarm is cleared from the keypad display.

This parameter causes an output to respond when a corresponding point with the same number is faulted.
Outputs used for this function must not be shared with any other point, keypad, sked, area, or panel output functions. Sharing can cause errors in output operation.
Reference
Points > Point Indexes > Output Response Type

Display as Device

Default: No
Selections: Yes/No
Use this parameter to cause the keypad to display CHECK DEVICE once a point is off normal or is acknowledged after going into alarm.
This parameter can be used for devices that have a dry contact output which faults a point once the device is in a trouble condition.
Yes: Display [CHECK DEVICE] when this point is off normal.
No: Do not display [CHECK DEVICE] when this point is off normal.
Reference
Points > Point Indexes > Display as Device

Local While Disarmed

Default:
- Point Indexes 1 to 8: No
- Point Index 9: Yes
- Point Indexes 10 to 11: No
- Point Index 12: Yes
- Point Indexes 13 to 31: No

Selections: Yes/No
Use this parameter to allow a controlled point to report alarms, troubles and restoral reports only when the area is armed. This parameter does not affect local annunciation.

IMPORTANT:
- This parameter suppresses all reports from 24-hour points. Do not use this parameter with Point Type set to 24-Hour. This parameter only works for disarmed points, and a 24 hour "always armed" point. Instead, choose any type other than 24-Hour, and use a point response that sends an alarm whether the point is armed or not. For instance, Point Type Part On and Point Response 9 send an alarm on a trouble or a short (I) whether the area is armed or not.
- A restoral report is transmitted even when the area is disarmed if the alarm or trouble event occurred while the area was armed and returned to normal after the area was disarmed.
- This parameter affects keyswitch points and suppresses keyswitch (troubles/restorals).
- To meet UL864 requirements for central station and remote station applications, set this parameter to **No**.

Yes: Suppress alarm, trouble and restoral reports from this point while the area it is assigned to is disarmed.
No: Report events occurring from this point while the area is disarmed.
Reference
Points > Point Indexes > Local While Disarmed

Local While Armed

Default: No
Selections: Yes/No
Use this parameter to allow a controlled point (Part On, Interior and Interior Follower), to report alarms, troubles and restoral reports only when the area is disarmed. This parameter does not affect local annunciation.

IMPORTANT:
- This parameter suppresses all reports from 24-hour points. This parameter only works for disarmed points, and a 24 hour "always armed" point. Instead, choose any type other than 24-Hour, and use a point response that sends an alarm whether the point is armed or not. For instance, Point Type Part On and Point Response 9 send an alarm on a trouble or a short (I) whether the area is disarmed or not.
- This parameter affects keyswitch points and suppresses keyswitch (alarms/troubles/restorals) and D279 (opening/closing/troubles/restorals) Do not use this parameter for controlled points that arm/disarm.
- To meet UL864 requirements for central station and remote station applications, set this parameter to **No**.

Yes: Suppress alarm, trouble and restoral reports from this point while the area it is assigned to is armed.
No: Report events occurring from this point while the area is armed.
Reference
Points > Point Indexes > Local While Armed

Disable Restorals

Default: No
Selections: Yes/No
Use this parameter to disable any restoral reports from this point after it returns to normal from an alarm or trouble condition.
IMPORTANT: To meet UL864 requirements for central station and remote station applications, set this parameter to **No**.
Yes: Disable restoral reports for this point.
No: Enable restoral reports for this point.
Reference
Points > Point Indexes > Disable Restorals

Force Arm Returnable

Default: No
Selections: Yes/No
Use this parameter to allow points which were force armed out of the area to return back to the armed state once they are normal again without needing to disarm the system.
Use this parameter on points assigned to loading dock doors that are required to be left open until loading is completed. Once the loading dock door is closed, it detects an opening and sends an alarm.
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.
Reference
Points > Point Indexes > Force Arm Returnable

Bypass Returnable

Default: No
Selections: Yes/No
Use this parameter to return a point which has been bypassed, force armed or swinger bypassed back into the system once the area this point is assigned to is disarmed.

IMPORTANT: Set this parameter to No for interlock points.

When not allowed to return to the system through disarming, the point must be manually unbypassed using the UNBYPASS?, keypad function, Sked functions Unbypass a point or Unbypass All Points, or remotely using RPS.

For force armed points to remain bypassed, ensure Force Arm Returnable is set to 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.

Reference

Points > Point Indexes > Bypass Returnable

Bypassable

Default: Yes

Selections: Yes/No

Use this parameter to allow this point to be bypassed and/or force armed.

When a 24-hour point or 24-hour supervisory point is bypassed, 24 HOUR BYPASS continuously scrolls on the keypad. FIRE BYPASS scrolls to indicate a 24-hour fire point or a fire supervisory point is bypassed. GAS BYPASS scrolls to indicate a gas detector or gas supervisory point is bypassed.

To have the alarm capability of a 24-hour point without the continuous scrolling, use a Part On point with a Point Response of 9 to E.

Setting this parameter to Yes for cross points can cause missed cross-point alarms. For example, if Points 1 and 2 are programmed as cross points and Point 1 is bypassed or force armed, Point 2 is not able to generate an ALARM CROSS POINT event. However, Point 2 can generate an UNVERIFIED or ALARM event depending on how the point was tripped.

A point can be bypassed at the keypad using the BYPASS? function, which reports as a `COMMAND BYPASS`. When bypassed by Sked function Bypass a Point, the report is `SKED BYPASS`. When bypassed by RPS, `RPS BYPASS` is sent after RPS disconnects from the control panel. When swinger-shunted, a `SWINGER SHUNT` is sent.

If the point is not bypassable, it cannot be bypassed in any of the above cases.

IMPORTANT:

- To meet UL864 requirements, set this parameter to **No**.
- This setting does not affect Service Bypass.

Yes: This point can be bypassed and force armed.

No: This point can not be bypassed or force armed from the keypad or RPS. However, it can be force armed by automatic arming at the end of the closing window (see Auto Close), or by a Sked programmed to arm the area.

RPS Menu Location

Points > Point Indexes > Bypassable

Swinger Bypass

Default: No

Selections: Yes/No

Use this parameter to allow the control panel to automatically bypass a point that erroneously reports a pre-determined number of alarm or trouble events within the same arm cycle. The Swinger Bypass Count parameter sets the maximum number of faults allowed on a point.

The control panel reports a Swinger Bypass when the Swinger Bypass Count is reached and Report Bypass at Occurrence is set to **Yes**. If the point has a partial

count (less than the Swinger Bypass Count number of events an hour), the count is reset to zero.
Bypassable does not need to be set to Yes for swinger bypass to work.
A swinger-shunted point returns to the system if Bypass Returnable is set to Yes. If not, return the point to the system as described in Bypass Returnable.
IMPORTANT: To meet UL864 requirements, set this parameter to **No**.
Yes: Enable Swinger Bypass for this point.
No: Disable Swinger Bypass for this point.
Reference
Points > Point Indexes > Swinger Bypass

Report Bypass at Occurrence

Default: No
Selections: Yes/No
This parameter allows a point to generate a COMMAND BYPASS report as soon as a user bypasses the point from the keypad. Enable this parameter for all bypassable 24-hour points. You can also report a bypassed point at the time the area is armed. See Defer Bypass Report.
Yes: Send a COMMAND BYPASS report at the time that the point is bypassed.
No: Do not send a COMMAND BYPASS report at the time the point is bypassed.
Reference
Points > Point Indexes > Report Bypass at Occurrence

Defer Bypass Report

Default: No
Selections: Yes/No
Use this parameter to prevent points that are bypassed by the user (COMMAND BYPASS)from occurring until the area is armed. Once the area is armed, the bypassed points as well as any point being bypassed during the arming sequence report as POINT BYPASS along with the closing report.
To report the bypass at occurrence and when the area is armed, set this parameter and Report Bypass at Occurrence to Yes. A COMMAND BYPASS report is sent as soon as it occurs, and a POINT BYPASS report is sent with the closing report.
WARNING:
- Bypass reports do not occur when arming the area if the closing report is suppressed by Open/Close windows, or are not being reported.
- Bypass reports for 24 hour points are not sent if this parameter and Report Bypass at Occurrence are both set to No.

Yes: Send a POINT BYPASS report with the closing report instead of a COMMAND BYPASS when the point is bypassed by a user.
No: Do not defer bypass reports.
Reference
Points > Point Indexes > Defer Bypass Report

Cross Point

Default: No
Selections: Yes/No

IMPORTANT:
- The Cross Point function is fixed to a maximum of two points per group. There are 31 available groups.
- Only use this parameter with non-fire points.

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 (see Cross Point Timer) from at least two points within a cross point group (see table below) before the system sends cross point alarm events. This parameter must be set to **Yes** for points to generate cross point alarm events.

The GV4 control panels support the following number of cross point groups:

- **D9412GV4:** 31 groups
- **D7412GV4:** 10 groups

Each cross point group consists of eight points, and is identified by the point numbers in them (for example, Cross Points 1-8, Cross Points 9-16, and so on).
A maximum of two points must be programmed to meet the cross point criteria.
Point numbers from different cross point groups do not affect each other.
When a point with this parameter set to **Yes** detects an alarm, the control panel starts the cross point timer. If a second cross point in the same cross point group detects an alarm while the cross point timer is active, the control panel sends cross point alarm events for both points.
A cross point is considered to be in alarm when it meets the criteria for instant alarm response. The cross point index must have Point Response set to a value that generates an instant alarm.
If a single cross point detects an alarm and stays faulted throughout the cross point timer, the system sends a standard alarm report for that point.
If a single cross point detects an alarm, then restores, and does not detect any other condition, the system sends an unverified event for that point. A second alarm on the first point does not create an alarm event, but rather an unverified 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 if the area is not disarmed in time.
The cross point function does not activate when a fault occurs on a controlled point (Point Types Part On, Interior and Interior Follower) in the disarmed, Entry Delay, or Exit Delay states.
If an abort window delay is needed for the cross zone alarm, all cross points in the group must have Alarm Abort set to **Yes**.

Cross Point Group	Point Range
1	1-8
2	9-16
3	17-24
4	25-32
5	33-40
6	41-48
7	49-56
8	57-64
9	65-72
10	73-80
11	81-88
12	89-96
13	97-104
14	105-112
15	113-120
16	121-127

Cross Point Group	Point Range
17	129-136
18	137-144
19	145-152
20	153-160
21	161-168
22	169-176
23	177-184
24	185-192
25	193-200
26	201-208
27	209-216
28	217-224
29	225-232
30	233-240
31	241-247

Reference
Points > Point Indexes > Cross Point

Alarm Verify

Default:
- Point Indexes 1 to 4: No
- Point Index 5: Yes
- Point Indexes 6 to 31: No

Selections: Yes/No
Yes: Enable alarm verification on this point.
No: Disable alarm verification on this point.
Use this parameter only with fire or gas points to designate them for alarm verification.
Alarm verification is a feature of automatic fire detection and alarm systems to reduce false alarms where sensors report alarm conditions for a minimum period of time, or confirm alarm conditions within a given period of time after being reset, in order to be accepted as a valid alarm initiation signal.

IMPORTANT:
- Do not enable the Cross Point Feature in Point Indexes that are designated for fire points.
- Check the sensor's datasheet for the stabilization time and enter a value at least 5 seconds higher than the longest time specified by any sensor in the loop.
- Check with your Authority Having Jurisdiction (AHJ) to determine the maximum verification time allowed.

Alarm verification points are programmed individually to activate the verification feature. Refer to *Point Index*. Any resettable fire point can activate alarm verification for the area to which it is assigned. Bosch recommends using separate area alarm verification outputs.
To enable alarm verification on a point, set Point Type to **Fire**, and Alarm Verify and Resettable to **Yes**.
When an alarm verification point is faulted, the control panel automatically removes power from all resettable points connected to the areas Reset Sensors output. Power is removed for 4.5 seconds. When power is reapplied, the control panel ignores alarms from resettable points for the amount of time programmed in Restart Time. After Restart Time has expired, a 65 second confirmation window begins. If the alarm verification point is still in alarm, or faults again during the confirmation window, or if a different alarm verification point in the area faults, an alarm is generated.
Reference
Points > Point Indexes > Alarm Verify

Resettable

Default:
- Point Indexes 1 to 3: No
- Point Indexes 4 to 5: Yes
- Point Indexes 6 to 31: No

Selections: Yes/No
Use this parameter if this is a powered point that requires interruption of power to reset a latched alarm condition. The resettable point function is typically used with smoke detectors and glass break detectors.
When initiated either through a Fire Walk Test or the keypad function RESET SENSOR?, or by RPS, power is interrupted to the device for 4-1/2 seconds. SENSOR RESET is reported to the central station receiver.

IMPORTANT:
- When a sensor reset is initiated, the control panel does not accept alarms from any points in which this parameter is set to Yes. During the 4-1/2 second reset time combined with restart time (configured in Restart Time), alarms or troubles from these points are ignored.
- Do not mix fire and intrusion devices on the same powered loop.
- To meet UL864 requirements, set this parameter to Yes for applicable resettable points.
- Setting this parameter to No prevents a resettable point from going back into alarm after an alarm annunciator reset.

Yes: This point is reset by the RESET SENSORS? function and during the alarm verification sequence.
No: This point is not resettable.
Reference
Points > Point Indexes > Resettable

Alarm Abort

Default:
- Point Indexes 2 - 6, 22, 31: No
- All others: Yes

Selections: Yes or No

This parameter allows points with the associated point index to delay a burglar alarm (non-fire) event for the time period specified in Abort Window.

An alarm is aborted by performing an alarm silence operation before this time elapses at a keypad showing the burglar alarm condition. When an alarm is successfully aborted, the keypad shows an optional `ALARM NOT SENT` message. See Abort Display for more information.

IMPORTANT:
- This parameter does not apply to fire alarms or invisible point alarms.
- To comply with UL standards, the total amount of time entered in Entry Delay and Alarm Event Abort must not exceed 1 minute.
- When upgrading a non-GV4 control panel account to a GV4 control panel account, RPS forces the default to **No**.

Yes: If the point goes into alarm, the system delays the alarm report for the amount of time specified in Abort Window.

No: If the point goes into alarm, the system immediately sends the alarm report.

Reference

Points > Point Indexes > Alarm Abort

Wireless Point Supervision Time

Default:
- **Point Indexes 1 to 2:** None
- **Point Indexes 3 to 6:** 4 hours
- **Point Indexes 7 to 19 and 21:** None
- **Point Index 20:** 24 hours
- **Point Index 22:** 4 hours
- **Point Indexes 23 to 24:** None
- **Point Indexes 25 to 31:** 24 hours

Selections: None, 4, 12, 24, 48, 72 hours

RPS supports the configuration of the Wireless Point Supervision Time for devices configured to report to the Wireless Receiver. **None** = no wireless point supervision, **4, 12, 24, 48, 78 hours** = hours between hearing from the wireless transmitter before sending a missing condition. Default setting is None

Notes

Wireless Point Supervision Time:
- Keyfobs will follow 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 the point type is Fire, then the Wireless Point Supervision Time setting can only be set to 4 hours.
- This is an alternate supervision interval to the global System Supervision Time setting.

Custom Function

Default: Disabled
Selections:
D9412GV4: Disabled, CF 128 to CF 143
D7412GV4: Disabled, CF 128 to CF 131
This specifies the custom function to be run when a point with this index faults to a short (S) or open (O) state.
RPS Menu Location
Points > Point Indexes > Custom Function

Monitor Delay

Default: 00:00
Selections: 00:00, 00:01 thru 60:00
00:00 = disabled
Use this parameter to configure the length of time (MM:SS) the control panel waits after a point faults before reporting the event to the central station.
The control panel sends a report to the central station if the point remains faulted during the entire period of time configured in this parameter. If the point is restored during this time, no report is sent. The control panel does not indicate when a report is sent.
Enable this feature to monitor a door, such as a freezer that should not be left open.
RPS Menu Location
Points >Point Indexes (point profiles) >Monitor Delay

Delay Response, Disarmed

Default: 00:00
Selections: 00:00, 00:05 thru 60:00
00:00 = disabled
This parameter sets the length of time (MM:SS) the control panel waits after a disarmed point faults before annunciating or reporting the fault. This parameter only applies to the following point types when disarmed:
Part On
Part On points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using Part Oning functions) separately from points programmed as interior. This lets the user partially arm the system to establish perimeter protection and still occupy the interior of the protected premises.
Part On points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.
When a Part On point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Part On point trips, the panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Part On point's entry delay time is less than the remaining time, it shortens the entry delay time.
Part On points programmed for an instant Point Response , generate an alarm immediately when tripped, even during entry or exit delay.
Interior
Interior points are armed only by arming All On the area. They are not armed when using Part Oning functions. These points are typically used to monitor interior

detection devices such as interior doors, motion detectors, photoelectric beams, and carpet mats.
Interior points can be either Instant or Delayed:

- **Instant:** Interior points are usually programmed for an instant alarm (see Point Response). Points programmed for instant alarms generate alarms immediately, even during entry or exit delay.
- **Delayed:** Interior Points can be programmed for a delayed Point Response . A delayed response means that if the point is tripped while the area is armed, it initiates entry delay. It does not generate an alarm until entry delay expires.

When an interior point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when the interior point trips, 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.
Delayed points can also initiate an entry tone at the keypad (see Entry Tone Off).
IMPORTANT: In some cases, you might need to create an interior point that causes an instant alarm only if entry delay protection is not tripped first. Use Interior Follower to create this type of protection.

Interior Follower

Interior follower points are armed only by all on arming the area. They are not armed when using Part Oning functions.
An interior follower point does not create an alarm if it trips while the area is in entry delay. An interior follower does not change the amount of remaining entry delay time. If no entry delay is in effect when the interior follower trips, it creates an instant alarm.
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 Entry Delay for an interior follower point.
IMPORTANT: It might be necessary to increase the Debounce count for interior follower points to prevent interior follower points from going into alarm before the control panel recognizes that a Part On delay point has been faulted. Program the interior follower point's Debounce for one number higher than the debounce count on Part On delay points.
Use this feature to delay the following parameters:

- Point Response
- Instant Alarm
- Supervisory
- Buzz on Fault
- Watch Point
- Output Response Type
- Display as Device
- Output

RPS Menu Location

Points > Point Indexes (point profiles) > Delay Response Disarmed

Delay Response Armed

Default: 00:00
Selections: 00:00, 00:05 thru 60:00
00:00 = disabled
This parameter sets the length of time (MM:SS) the control panel waits after an armed point faults before annunciating or reporting the fault. This parameter only applies to the following point types when armed:

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 panic, medical, and police alerts.

24-hour points can be programmed as bypassable. However, the application should be carefully considered before using the bypassable option. Bypassable 24-hour points should be programmed to Buzz on Fault.

When a 24-hour point is bypassed, the report should be sent as it occurs. If the area contains all 24-hour points, the area is never armed or disarmed; therefore, a deferred bypass report is not sent.

24-hour protection for fire doors, roof hatches, etc. Instead of programming this type of protection as a 24-hour point, consider using a Part On point type with a Point Response of 9 to E. 24-hour points do not show faults when an arming function is entered, but Part On points do. When programming for this type of protection, you should consider using the Buzz On Fault and Local While Disarmed options.

Part On

Part On points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using Part Oning functions) separately from points programmed as interior. This lets the user partially arm the system to establish perimeter protection and still occupy the interior of the protected premises.

Part On points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.

When a Part On point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Part On point trips, the panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Part On point's entry delay time is less than the remaining time, it shortens the entry delay time.

Part On points programmed for an instant Point Response , generate an alarm immediately when tripped, even during entry or exit delay.

Interior

Interior points are armed only by arming All On the area. They are not armed when using Part Oning functions. These points are typically used to monitor interior detection devices such as interior doors, motion detectors, photoelectric beams, and carpet mats.

Interior points can be either Instant or Delayed:

- **Instant:** Interior points are usually programmed for an instant alarm (see Point Response). Points programmed for instant alarms generate alarms immediately, even during entry or exit delay.
- **Delayed:** Interior Points can be programmed for a delayed Point Response . A delayed response means that if the point is tripped while the area is armed, it initiates entry delay. It does not generate an alarm until entry delay expires.

When an interior point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when the interior point trips, 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.

Delayed points can also initiate an entry tone at the keypad (see Entry Tone Off).

IMPORTANT: In some cases, you might need to create an interior point that causes an instant alarm only if entry delay protection is not tripped first. Use Interior Follower to create this type of protection.

Interior Follower

Interior follower points are armed only by all on arming the area. They are not armed when using Part Oning functions.

An interior follower point does not create an alarm if it trips while the area is in entry delay. An interior follower does not change the amount of remaining entry delay time. If no entry delay is in effect when the interior follower trips, it creates an instant alarm.
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 Entry Delay for an interior follower point.
IMPORTANT: It might be necessary to increase the Debounce count for interior follower points to prevent interior follower points from going into alarm before the control panel recognizes that a Part On delay point has been faulted. Program the interior follower point's Debounce for one number higher than the debounce count on Part On delay points.
Use this feature to delay the following parameters:
– Point Response
– Instant Alarm
– Supervisory
– Output Response Type
– Display as Device
– Output

RPS Menu Location
Points > Point Indexes (point profiles) > Delay Response Armed

11.2 Point Assignments

Point Source

Default: Onboard for points1 to 8, **Unassigned** all others
Selections: Unassigned, Zonex, Octo-input, Wireless, Onboard, Door Point
– **Unassigned**. Point is not installed.
– **Zonex**. Point is assigned to a Zonex bus input module. Including Zonex RF point.
– **Output**. Logical connection to the output of the same number.
– **Octo-input**. Point is assigned to an SDI2 bus input module.
– **Wireless**. Point is assigned to an SDI2 bus RF receiver.
– **Onboard**. Point is assigned to a control panel.
– **Door Point**. Point is assigned to an SDI bus Door Controller. Not selectable here.

This parameter indicates to the control panel the device each point is assigned to. The Point Source selection dialog box allows selection of only the options available for the point number. When a selection is grayed out, that option is not allowed when configuring that particular point.
IMPORTANT:
– Point numbers 128 and 248 are reserved for Zonex bus 1 and bus 2 statuses.
– Any point location (including onboard) may be overridden by the access controller configuration (Door Point).
– The Door Point option for 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.
– Point number 128 is reserved for supervising Zonex 1.
– Point number 248 is reserved for supervising Zonex 2 (D9412GV4).

RPS Menu Location
Points > Point Assignments > Point Source

Point Text

Default:
D9412GV4:
- **Point 1:** Fire
- **Point 2:** Entry/Exit Delay
- **Point 3:** Entry/Exit Delay
- **Point 4:** Interior Follower
- **Point 5:** Interior Follower
- **Point 6:** Part On Instant
- **Point 7:** Part On Instant
- **Point 8:** 24 hour
- **Point 9 to Point 247:** Point Text

D7412GV4
- **Point 1:** P1 Fire
- **Point 2:** P2 Panic
- **Point 3:** P3 Delay
- **Point 4:** P4 Follow
- **Point 5:** P5 Instant
- **Point 6:** P6 Instant
- **Point 7:** P7 Instant
- **Point 8:** P8 Instant
- **Point 9 to Point 28:** (point #)

Selections: Up to 32 alphanumeric characters.
This parameter sets what is displayed at keypads (if the point is programmed as "visible") and reported to the central station receiver when transmitting in Modem4 format (if it is a reporting point).
Enter up to 32 characters of text to describe the point.
- SDI2 keypads display the first 20 characters. If more than 20 characters are used, the text scrolls across the display one time. To scroll the text again, press [ESC].
- Spaces before, after and within a string of text are treated as text and are included in the 32 character limit.
- On SDI keypads, only the first 16 characters display.

Note: Include the point number in custom point text. This helps the user when viewing events, initiating bypasses, etc. and can simplify troubleshooting.
Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2.
The D9412GV4 supports Points 1 to 247. The D7412GV4 supports Points 1 to 75.
RPS Menu Location
Points > Point Assignments > Point Text

Point Index

Default: (click on the panel versions below to see the default settings for each panel version. To lookup the current settings of a particular Point Index go to POINTS > Point Indexes **)**

- **D9412GV4**
- Point 1: 4
- Point 2: 8
- Point 3: 25
- Point 4: 13
- Point 5: 13
- Point 6 and 7: 7
- Point 8: 0
- Points 9 to 127: 0
- Point 128: (Not Used)
- Points 129 to 247: 0
- **D7412GV4**
- Point 1: 3
- Point 2: 1
- Point 3: 8
- Point 4: 13
- Point 5 to 8: 7
- Points 9 to 75: 0

Selections: 0 to 31

This entry selects one of the 31 point index codes that define the points' characteristics and determine how the control panel responds to various point conditions.

0 (zero) disables the point.

MISSING POINT reports occur if a point address does not exists for a point that is assigned a point index. EXTRA POINT events occur if more than two devices have the same address. EXTRA POINT events also occur if a device is addressed but has no programming (Point Index = 0). For example, installing a D9210C door control but not assigning a door point.

When a POPIT goes 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 that have a Point Response of 9 - D will generate a Missing Alarm response while disarmed.

POPIT modules monitor their sensor loops for three conditions, loop normal, loop open, and loop shorted. They report these three conditions to the control panel. The panel uses point programming to interpret the sensor loop information reported by the POPITs and make the appropriate system response.

IMPORTANT

- Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2.
- The D9412GV4 supports Points 1 to 247. The D7412GV4 supports Points 1 to 75.

Reference

Points > Point Assignments > Point Index

Point Index Description

Selections: No selections – this field cannot be edited by the user.
This field displays a description of the point index that is entered in the Point Index Description field. It is a reference field only and the information displayed in it is not sent to the control panel.

IMPORTANT:
– Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2.
– The D9412GV4 supports Points 1 to 247. The D7412GV4 supports Points 1 to 75.

Reference
Points > Point Assignments > Point Index Description

Area

Default: 1
Selections:
– D9412GV4: 1 to 32
– D7412GV4: 1 to 8
The areas are numbered 1 to 32. Select the area number to which the point will be assigned.

IMPORTANT:
- Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2.
- The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.

Reference
Points > Point Assignments > Area

Debounce

Default: 2
Selections: 1-15

Scans	Debounce	Scans	Debounce	Scans	Debounce
1	410 ms	6	2.46 s	11	4.51 s
2	820 ms	7	2.87 s	12	4.92 s
3	1.23ms	8	3.28 s	13	5.33 s
4	1.64 s	9	3.69 s	14	5.74 s
5	2.05 s	10	4.10 s	15	6.15 s

The debounce count is the number of times the control panel scans a point before initiating an alarm. Scan cycles are 410 ms.
For appropriate settings, consult the manufacturer's instructions for the device connected to this point.

IMPORTANT:
- Bosch recommends that points assigned to D9210C modules have a debounce of 4. Interior follower points should have a debounce of at least three. All others should have an entry of 2 or higher.

- Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2.
- The D9412GV4 supports Points 1 to 247. The D7412GV4 supports Points 1 to 75.
- Debounce does not apply to wireless points. RPS automatically selects a dash (-) for Debounce, which indicates that Debounce is not applicable.

RPS Menu Location
Points > Point Assignments > Debounce

Output

Default: 0
Selections: 0 to 8 (increments of 1)
Use this parameter to activate an output when the point goes into alarm.
The output does not activate for Trouble nor Supervisory events. Reset the output by clearing the memory from the keypad display.
The outputs used can be on an output module installed on either the Zonex bus or the SDI2 bus.

Output Code	D9412GV4 Output	D7412GV4 Output
0	disabled	disabled
1	73	9*
2	74	10
3	75	11
4	76	12
5	77	13
6	78	14
7	79*	15
8	80*	16

*These outputs are only available on Zonex output modules.
RPS Menu Location
Points > Point Assignments > Output

RFID (B820 Inovonics Wireless)

Default: 0 (When the Point Source is configured to Wireless)
Selections: 0 - 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.

IMPORTANT: If an SDI2 communication device is allocated for automation communication, then it cannot be used for central station nor for RPS communication.

Reference

Points > Point Assignments > RFID (B820 Inovonics Wireless)

RFID (B810 RADION Wireless)

Default: 0 (When the Point Source is configured to Wireless)

Selections: 0 - 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.

IMPORTANT: If an SDI2 communication device is allocated for automation communication, then it cannot be used for central station nor for RPS communication.

Reference

Points > Point Assignments > RFID (B810 RADION Wireless)

RADION Point Device Type

Default:

- If no wireless device is selected: (-)
- If a wireless device is selected: Wireless Door Window Contact

Selections:

- Wireless Glass Break
- Wireless Smoke
- Wireless Inertia
- Wireless Door Window Contact
- Wireless Recessed Door Window
- Wireless Motion Dual
- Wireless Motion PIR
- Wireless Ceiling Mount Motion
- Wireless Universal TX
- Wireless Bill Trap
- Wireless Curtain Motion
- Wireless CO Detector
- Wireless Panic, One Button
- Wireless Panic, Two Button

This parameter allows point source options to be set to wireless.

If the wireless module type, is set to B810 Wireless Device, there is no limit on how many Point Source options can be set to wireless. (Note, even with keyfob supervision enabled, the wireless device should support 1800 devices.)

Each wireless device contains corresponding input functions. Enable or disable input functions by clicking the corresponding checkbox in the dialog box,

Device Type	Input 1	Input 2	Input 3	Input 4
Wireless Glass Break	Glass Break Alarm	Not Used	Not Used	Not Used
Wireless Smoke	Smoke Alarm	Not Used	Not Used	Not Used
Wireless Inertia	Reed Alarm	Loop Input	Vibration Alarm	Not Used
Wireless Door Window Contact	Reed Alarm	Not Used	Not Used	Not Used
Wireless Recessed Door Window	Reed Alarm	Not Used	Not Used	Not Used
Wireless Motion Dual	Motion Alarm	Not Used	Not Used	Not Used
Wireless Motion PIR	PIR Alarm	Not Used	Not Used	Not Used
Wireless Ceiling Mount Motion	Motion Alarm	Not Used	Not Used	Not Used
Wireless Universal TX	Reed Alarm	Loop Input	Not Used	Not Used
Wireless Bill Trap	Bill Trap Alarm	Not Used	Not Used	Not Used
Wireless Curtain Motion	PIR Alarm	Not Used	Not Used	Not Used
Wireless CO Detector	CO Alarm	Not Used	Not Used	Not Used
Wireless Panic, One Button	Not Used	Not Used	Not Used	Not Used
Wireless Panic, Two Button	Not Used	Not Used	Not Used	Not Used

Each point device must have at least one valid input function selected.
RPS will reset this field to the default value when the wireless device type is changed.

RPS Menu Location

Points > Point Assignments > RADION Point Device Type

11.3 Cross Point Parameters

Cross Point Timer

Default: 20
Selections: 5 - 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.
IMPORTANT: Only use the Cross Point function on non-fire points.
Reference
Points > Cross Point Parameters > Cross Point Timer

12 Schedules

12.1 Open/Close Windows

Opening/Closing Overview

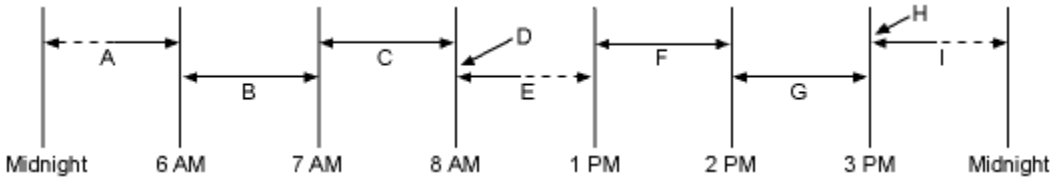
Use these windows to set a schedule for disarming and arming. The disarming and arming schedules provide several independent features:

- Suppress normal opening and/or closing reports when Disable O/C in Window is set to Yes.
- Generate a FAIL TO OPEN report if the area is not disarmed on schedule when Fail To Open is set to Yes.
- Provide a warning tone and [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 Fail To Close is set to Yes.
- Automatically arm the area at the end of the closing window when Auto Close is set to Yes.

Opening and closing schedules can be set up independently. For example, if you only want to use features provided by closing windows, leave times blank in the opening windows prompts and program closing window times.

Opening Window Timeline

Example using two opening windows on the same day



A. Areas that are disarmed between midnight and 6 AM generate Opening reports.
B. Areas that are disarmed between 6 AM and 7 AM generate Early to Open reports.
C. If the area is disarmed between 7 AM and 8 AM regular Opening Reports are generated. If Disable O/C in Window is programmed as "yes" the Opening Report is not transmitted to the central station.
D. If the area is not disarmed by 8:01 AM then a Fail to Open event is generated if Fail to Open is programmed as "yes" in Opening and Closing Options.
E. If the user disarms the area between 8:01 AM and 12:59 PM then a Late to Open event is generated.
F. Areas that are disarmed between 1 PM and 2 PM generate Early to Open reports.
G. If the area is disarmed between 2 PM and 3 PM regular Opening Reports are generated. If Disable O/C in Window is programmed as "yes" the Opening Report is not transmitted to the central station.
H. If the area is not disarmed by 3:01 PM then a Fail to Open event is generated if Fail to Open is programmed as "yes" in Opening and Closing Options.
I. If the user disarms the area between 3:01 PM and 11:59 PM then a Late to Open event is generated.

Programming for two Opening Windows on the same day (as shown in the time line)

			OPEN		CLOSE			
W#	Day of Week	Early Begin	Start	Stop	Early Begin	Start	Stop	Except On Holiday
1	S **M** T W T F S	06:00	07:00	08:00				Yes/**No**
2	S **M** T W T F S	13:00	14:00	15:00				Yes/**No**

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 have to 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 the example below:

Programming to Link Two Days Over Midnight

			OPEN		CLOSE					
W#	Day of Week	Early Begin	Start	Stop	Early Begin	Start	Stop	Except on Holiday	Holiday Index	Area(s)
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

Monday to Friday, opening between 5 and 6 AM, closing between 11 PM and 1 AM.

		OPEN			CLOSE			
W#	Day of Week	Early Begin	Start	Stop	Early Begin	Start	Stop	Except on Holiday
1	S **M T W T F** S	04:00	05:00	06:00	20:00	23:00	23:59	Yes/**No**
2	S M **T W T F** S	_ _ : _ _	_ _ : _ _	_ _ : _ _	00:00	00:00	01:00	Yes/**No**

Sunday, in between 8 and 8:30 AM, out between 2:30 and 5:00 PM.

		OPEN		
W#	Day of Week	Early Begin	Start	Stop
4	S M T W T F S	07:00	08:00	08:30
	All days must be programmed NO	Only on holidays.		

Opening/Closing Windows Table

Use this table to determine the proper entries for your application.

Day of Week	The column below briefly describes the ways to activate an Opening/Closing Window. use the guidelines shown in the other columns to choose the appropriate entries.	Except on Holiday	Holiday Index	Areas
Program at least one day as YES	Day(s) of the Week	NO	None	Program at least one Area as YES.
Program at least one day as YES	Day(s) of the Week, but NOT on Holidays	YES	Select at least one Index	Program at least one Area as YES
Program at least one day as YES	Day(s) of the Week, PLUS Holidays	NO	Select at least one Index	Program at least one Area as YES
All days must be programmed NO.	Only on Holidays	NO	Select at least one Index	Program at least one Area as YES

Sunday through Saturday (O/C Windows)

Default (Sunday through Saturday): No

Selections: Yes/No

In the seven weekday parameters, select the days of the week that the opening and/or closing windows are active.

To prevent the windows from activating on certain days of the year, set Xept Holiday to Yes, and enable at least one holiday index. When Xept Holiday is set to Yes, the window executes on the days of the week programmed unless the date is designated as a holiday by the selected holiday index.

If opening and/or 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, set Xept Holiday to No, and select a holiday index with the days of the year you want the window to be active.

Reference

Schedules > Open/Close Windows > Sunday through Saturday

Open Early Begin

Default: 00:00

Selections: HH:MM (hours and minutes) 00:00 to 23:59

This parameter is one of three required to create an opening window. To finish programming an opening window, Open Window Start and Open Window Stop also must be programmed.

The time entered in this parameter is the earliest time that the user is allowed to open an area before the Open 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 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).

IMPORTANT:

- Avoid programming the Open Early Begin time before a time that is between another window's Open Window Start and Open Window Stop times.
- Do not program a window to cross the midnight boundary.

Disabled windows have a 00:00 beginning time. If the entry for this parameter 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.

IMPORTANT: Ensure time entries use a 24-hour clock. For example, midnight = 00:00; 7:00 AM = 07:00; 2:45 PM = 14:45; 11:59 PM = 23:59.

If the window needs to activate on the same day you program it, reboot the control panel to activate today's window.

Reference

Schedules > Open/Close Windows > Open Early Begin

Open Window Start

Default: 00:00
Selections: HH:MM (hours and minutes)
Enter the time that you want the control panel to start the opening window. The window goes into effect at the beginning of the minute.
00:00 is Midnight 23:59 is 11:59 P.M. 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 parameter 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.
See Open Early Begin for report feature explanations.
Reference
Schedules > Open/Close Windows > Open Window Start

Open Window Stop

Default: 00:00
Selections: HH:MM (hours and minutes)
Enter the time that you want the control panel to end the opening window. The window stops at the end of the minute.
00:00 is Midnight 23:59 is 11:59 P.M. 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 parameter 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 panel generates a `FAIL TO OPEN` report if enabled in Fail To Open .
Opening reports generated between the Open Window Start time and Open Window Stop time can be suppressed by setting Disable O/C in Window to Yes. See Open Early Begin for other report feature explanations.
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.
Reference
Schedules > Open/Close Windows > Open Window Stop

Close Early Begin

Default: 00:00
Selections: HH:MM (hours and minutes) 00:00 to 23:59
This parameter 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 entered in this parameter is the earliest time the user can close an area before the Close Window Start time. If opening and closing reports are enabled, arming the area between midnight and the time entered in this parameter generates a closing report.

– If 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 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).

IMPORTANT: Avoid programming the Open Early Begin time that is between another window's Open Window Start and Open Window Stop times.

Disabled windows have a 00:00start time. If the entry for this parameter 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.

IMPORTANT: Ensure time entries use a 24-hour clock. For example, midnight = 00:00; 7:00 AM = 07:00; 2:45 PM = 14:45; 11:59 PM = 23:59.

If the window needs to activate on the same day you program it, reboot the control panel to activate today's window.

Reference

Schedules > Open/Close Windows > Close Early Begin

Close Window Start

Default: 00:00

Selections: 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 P.M. 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 parameter 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.

A warning tone sounds and [PLEASE CLOSE NOW] displays at the keypad if the area is not armed when the Close Window Start time comes. To temporarily silence the tone, press the [ESC] key on the keypad. The warning tone restarts in 10 minutes if the area is not armed.

See Close Early Begin for report feature explanations.

Reference

Schedules > Open/Close Windows > Close Window Start

Close Window Stop

Default: 00:00

Selections: 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 P.M. 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 parameter 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 setting Disable O/C in Window to Yes. See Close Early Begin for other report feature explanations.
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 have to 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:

			OPEN		CLOSE			
W#	Day of Week	Early Begin	Start	Stop	Early Begin	Start	Stop	Except On Holiday
1	**S M T W T** F S				22:00	23:30	23:59	Yes/**No**
2	S **M T W T F** S				00:00	00:00	00:30	Yes/**No**

RPS Menu Location
Schedules > Open/Close Windows > Close Window Stop

Xept on Holiday (O/C Windows)

Default: No
Selections: Yes/No
This parameter allows you to 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, set Xept Holiday to Yes, and enable at least one holiday index. When Xept Holiday is set to Yes, the window executes on the days of the week programmed unless the date is designated as a holiday by the selected holiday index(es).
To use this parameter, the window must be programmed to activate on at least one day of the week and a holiday index must be enabled.
You also use this selection if opening and/or 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, set Xept Holiday to No, and select at least one holiday index with the days of the year you want the window to be active.
See Holiday Indexes for O/C Windows for more information.
Yes: Do not activate this window on holidays.
No A holiday does not prevent this window from activating.
Reference
Schedules > Open/Close Windows > Xept on Holiday

Holiday 1 to Holiday 4 (O/C Windows)

Default (Holiday 1 through Holiday 4): No
Selections: Yes/No
You can enable up to four holiday indexes for use with opening/closing windows. Enable at least one holiday index if Xept Holiday is set to Yes for this window, or if you want this window to activate only on specific dates.
Yes: Use the selected holiday index with this window.
No: Do not use the selected holiday index with this window.
Reference
Schedules > Open/Close Windows > Holiday 1 to Holiday 4

Area 1-32

Default: No
Selections: Yes/No
Eight separate parameters determine whether a particular window activates in each of the control panel's eight areas.
IMPORTANT: The D9412GV4 supports up to 32 areas, the D7412GV4 supports up to 8 areas.
Yes Activate the window in the specified area number.
No Disable the window in the specified area number.
Reference
Schedules > Open/Close Windows > Area 1-32

12.2 User Group Windows

User Group Windows Overview

In this section, you can create up to eight User Group periods in which the passcodes for the group chosen will be enabled. One user group can have multiple windows assigned to them within a 24 hour period. See User Group, in the Passcode Worksheet section of the program to assign individuals to a group.
When you assign a 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 Window #.
If a user is not assigned to a User Group or the number programmed for the user for User Group is not assigned to a User Window # , the passcode for that user is enabled all the time.
IMPORTANT: User Group Windows do not affect the users token/card access authority. To enable/disable tokens, Token Levels On/Off.

User Group

Default: 1
Selections: 0 (Blank), 1 to 8
Enter the number programmed for the group of users in this parameter. This group will have their user passcodes enabled/disabled when this window runs.
IMPORTANT: 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.
Reference
Schedules > User Group Windows > User Group

Sunday through Saturday (User Group Windows)

Default (Sunday through Saturday): No
Selections: Yes/No
In the seven weekday parameters, select the days of the week that the User Group window is active.
To prevent the windows from activating on certain days of the year, set Xept Holiday to Yes, and enable at least one holiday index. When Xept Holiday is set to Yes, the window executes on the days of the week programmed unless the date is designated as a holiday by the selected holiday index.
If opening and/or 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, set Xept Holiday to No, and select a holiday index with the days of the year you want the window to be active.
Reference
Schedules > User Group Windows > Sunday through Saturday

Group Enable Time

Default: 00:00
Selections: HH:MM (hours and minutes)
IMPORTANT: This parameter must programmed if this User Group Window is assigned to a user group.
Enter the time of day that the window starts. Beginning at this time, users assigned to this window's group are allowed to 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).
When disabling Group Enable Time input, the time reverts back to 00:00.
Perform a Reset Panel command when ending the communications session to activate today's window. If you are programming a window that needs to activate on the same day that you are programming it, do a Reset Panel command after programming.
Reference
Schedules > User Group Windows > Group Enable Time

Group Disable Time

Default: 00:00
Selections: HH:MM (hours and minutes)
IMPORTANT: This parameter 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 = 07:00, 2:45 PM = 14:45.
To disable the window, both the hours and minutes spaces must be blank.
Do not program a single window to cross the midnight boundary. The window stop time must be later than the window start time.
Reference
Schedules > User Group Windows > Group Disable Time

Xept Holiday (User Group Windows)

Default: No
Selections: Yes/No
This entry allows you to determine if the window is disabled on holidays, or is active only on holidays. Use the instructions provided in W# Xept Holiday .
Reference
Schedules > User Group Windows > Xept Holiday

Holiday 1 to Holiday 4

Default (Holiday 1 through Holiday 4): No
Selections: Yes/No
You can enable up to four holiday indexes to use with User Group Windows.
Enable at least one holiday index if Xept Holiday is set to Yes for this User Window, or if you want this window to activate only on specific dates.
Yes: Use the selected holiday index with this window.
No: Do not use the selected holiday index with this window.
Reference
Schedules > User Group Windows > Holiday 1 to Holiday 4 or
Schedules > Skeds > Holiday 1 to Holiday 4

12.3 Skeds

Skeds — Overview

Use the SKEDS module to program the control panel to automatically execute functions-that are otherwise initiated 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 Time Edit is set to **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 Function. A function is what is executed. In addition to the function, a choice must be made to what is affected by the function. (e.g. When choosing a Disarm Sked, the disarming is the function while the areas that are being chosen to become disarmed are what is affected).
The functions and their associated parameters are explained in detail following the Function prompt.
Each Sked can be programmed with up to four Holiday Indexes. The Holiday Indexes can be used to execute the Sked on the Holidays in addition to the Date or Day(s) of the Week, or, they can be used to prevent the Sked from executing on the Holidays (see Xept Holiday).

Sked Descriptions

Default: Blank
Selections: Up to 24 alphanumeric characters
Enter up to 24 characters of text to describe the area. This is for informational purposes only and is not sent to the control panel.
Reference
Schedules > Skeds > Sked Descriptions

Time Edit

Default: Yes
Selections: Yes/No
Select whether the user can edit the time of this Sked from the keypad.
- Yes: The user can edit the time of this Sked from the keypad, and it appears in the CHANGE SKED display.
- No: The user cannot edit the time of this Sked from the keypad, and it does not appear in the CHANGE SKED displays.

Reference
Schedules > Skeds > Time Edit

12.3.1 Function

Default: Not in Use
Selections: Refer to list below.
Select the Function Name from the drop down list that you want this Sked to execute. The programmer automatically displays the available parameter choices and range fields for this function. (e.g. A list of check boxes are automatically displayed for the areas when choosing the arm/disarm function.

See below for information on each Sked function.

Not In Use
This function is disabled.
All On Delay
This function simulates the [ALL ON DELAY] keypad function. Entries in the 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 FA/Bypass max.
- D9412GV4 Arm Area allows entries up to 32 areas in Parameter 1: Area#
- D7412GV4 Arm Area allows entries up to 8 areas in Parameter 1: Area#

All On Instant
This function simulates the [ALL ON INSTANT] keypad function. Entries in the 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 FA/Bypass max.
- D9412GV4 Arm Area allows entries up to 32 areas in Parameter 1: Area#
- D7412GV4 Arm Area allows entries up to 8 areas in Parameter 1: Area#

Part On Delay
This function simulates the [PART ON DELAY] keypad function. Entries in the 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 FA/Bypass max.
- D9412GV4 Arm Area allows entries up to 32 areas in Parameter 1: Area#
- D7412GV4 Arm Area allows entries up to 8 areas in Parameter 1: Area#

Part On Instant
This function simulates the [ALL ON INSTANT] keypad function. Entries in the 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 FA/Bypass max.
- D9412GV4 Arm Area allows entries up to 32 areas in Parameter 1: Area#

– D7412GV4 Arm Area allows entries up to 8 areas in Parameter 1: Area#

Disarm

This function emulates the [DISARM] keypad function. Entries in the S## Area # prompts define the area(s) this Sked disarms. The Sked can disarm multiple areas.

– D9412GV4 Disarm Area allows entries up to 32 areas in Parameter 1: Area#
– D7412GV4 Disarm Area allows entries up to 8 areas in Parameter 1: Area#

Extend Close

This function sets the closing window start time to the current time plus the number of minutes configured in Parameter 1. This function can only take effect after the Close Early Begin time has passed.

NOTE: Extend Close time cannot extend past midnight. Furthermore, if enabled, it cannot extend past an area's configured Latest Close Time.

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 P## Bypassable is programmed YES in the Point Index assigned to the point. The bypass is reported if Bypass Reports are enabled in the Point Index assigned to the point. The Sked can bypass one point.

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.

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.

– D9412GV4 Unbypass Individual Point allows entries up to 32 areas in Parameter 1: Area#
– D7412GV4 Unbypass Individual Point allows entries up to 8 areas in Parameter 1: Area#

Set Output

This function emulates the [CHG OUTPUT?] keypad function to turn outputs ON. The entry in the Output Number parameter defines the specific output this Sked activates. The Sked can activate one output.

Reset Outputs

This function emulates the [CHG OUTPUT?] keypad function to turn outputs OFF. The entry in the Output Number parameter defines the output this Sked turns off. The Sked can turn off only outputs that were set by a Sked. The Sked can turn off one output.

Toggle Output

This function turns off the configured output if it is currently on or turns on the configured output if it is currently off. The entry in the Output Number parameter defines the specific output this sked toggles. This sked can only be use with one output.

Reset All Outputs

This function is not available as a keypad function. This Sked function turns off all outputs that were turned on by a Sked. This is a panel-wide function.

There are no other parameters that require input for this option.

Unlock Door
This function emulates the [UNLOCK? 12345678] keypad function for unlocking a door.
Lock Door
This function returns an Unlocked (function 18) or Secured (function 19) door to a normal locked door state.
Secure Door
This function emulates the [SECURE? 12345678] keypad function for securing a door.
Access Level
This function emulates the [ACCESS CMD LEVEL] command which determines whether a users token/card level will be enabled or disabled thus allowing them to have Access Granted rights. This affects all doors that this user is assigned to with this specific authority level. This function allows access to be turned on or off for the levels programmed.

IMPORTANT: 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/disable authority level 1 for door 1 without affecting his authority level for doors 2 through 8).

Access Granted Events On
The control panel can log Access Granted events when a valid token, "request to enter" (RTE), "request to exit" (REX), or "unlock door" event is detected for a specific door. These events can be directed to report remotely through Phone Routing. This Sked enables or disables Access Granted events to be reported for Door #.
The 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 report remotely through Phone Routing. This Sked enables or disables No Entry events to be reported for Door #.
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 panel is unpredictable.

IMPORTANT:

- Do not program multiple Skeds to execute at the same keypad during the same time of execution.
- Do not program Skeds to execute at times when a user is likely to be executing functions at the keypad.

Contact RPS User Port
This function attempts to contact Unattended RPS at the configured time over a network communication device at the configured port. The control panel's account in RPS controls the operations performed upon successful contact.
Send 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 Phone Routing. The status report can be deferred if any other report was sent since the last status report. To defer the status report for up to 24 hours, set the Defer Status option to Yes.

Send Test Report
This function emulates the [TEST REPORT?] keypad function. This function generates a test report ONLY from Area 1 but contains panel wide status information. The report is sent based on the Report Routing configuration under Panel Wide Parameters > Report Routing > Test Reports > Test Report.

With GV4 Series control panels, this function sends the following report to the central station:

Modem Event	Contact ID Event	Contact ID Code
Test Report – System normal, expanded status	Periodic Test Report	1 602 00 000

If Expand Test Report in Panel Wide > Phone and Phone Parameters is programmed Yes, the test report also includes all off-normal states for events listed in Panel Wide Parameters > Report Routing > Diagnostic Reports and Test Reports.

Parameter 1: Deferred
The test report can be deferred if any other report was sent since the last test report. To defer the test report for up to 24 hours, set the Parameter 1: Deferred option to Yes.

The test report can be sent hourly, monthly, or at a scheduled time. Select the desired frequency in Parameter 2.

Parameter 2: Frequency
Hourly. The Test Report will be sent every hour beginning at the time scheduled in Time.
Monthly, The Test Report will be sent every month on the same date beginning on the date and time scheduled in Date and Time.
Scheduled. The Test Report will be sent on the date and time scheduled in Date and Time.

IMPORTANT: To meet UL864 requirements, use the Sked function to meet the daily test report requirement.

Send Test on Off Normal
In order 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 events for any points that are in an off-normal state at the time the report is generated.
With GV4 Series control panels, this function sends the following report to the central station if the point is in an off-normal state:

Modem Event	Contact ID Event	Contact ID Code
Test Report – System off-normal, expanded status	Periodic Test – System Trouble Present	1 608 00 000

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.

Watch On
This function disables watch mode in the areas programmed in Parameter 1. Watch Mode causes the Watch Tone to sound at all keypads with scope to the enabled areas when a Watch Point is faulted.

Watch Off

This function disables watch mode in the areas programmed in Parameter 1. Watch Mode causes the Watch Tone to sound at all keypads with scope to the enabled areas when a Watch Point is faulted.

Show Date & Time

This function emulates the keypad shortcut Show Date/Time (MENU 523) for the keypads programmed in parameter 1. When enabled, the idle text of the indicated keypads will show the current date and time.

Sound Watch Tone

This function sounds the Watch Tone at the keypads programmed in Parameter 1. The Watch Tone sounds at all Keypads with the address programmed. Press ESC to silence the tone.

The D9412GV4/D7412GV4 Watchtone allows entries up to 16 Keypads Parameter 1: KP#

Set Keypad Volume

This function sets the configured keypads to the configured volume level at the scheduled time. Refer to Keypad Volume parameter in the keypad configuration section for details on volume parameters.

Set Keypad Brightness

This function sets the configured keypads to the configured brightness level at the scheduled time. Refer to Keypad Brightness parameter in the keypad configuration section for details on the brightness parameter.

Execute Custom Command

This function executes the configured custom function at a scheduled time.

Reference

Schedules > Skeds > Function

Time

Default: Disable

Selections: Disable, 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 display "Disabled" in the Time cell.

Follow these steps to program a time:

1. Double-click on the field corresponding to the Sked you are programming the time for.If "Disable" is checked, uncheck it. The time field will become active.
2. Click inside the time field and either use the up and down arrows to set the time, or type in the desired time.
3. Click on OK.

Follow these steps to Disable a Sked:

1. Double-click on the field corresponding to the Sked you wish to disable.
2. Select "Disable".
3. Click on OK.

Reference

Schedules > Skeds > Time

Date

Default: Disable
Selections: Disable, MM:DD (month and date)
Enter the date that the Sked executes. Disabled Skeds display "Disabled" in the Date cell.
Reference
Schedules > Skeds > Date

Sunday through Saturday (Skeds)

Default (Sunday through Saturday): No
Selections: Yes/No
These seven day of the week prompts select the days of the week that the Sked is active.
Exceptions:
To prevent the Sked from activating on certain days of the year, set Xept Holiday to Yes, and enable at least one holiday index. When Xept Holiday is set to 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 any days of the week. Instead, set Xept Holiday to No, and select a holiday index with the dates you want the window to be active.
IMPORTANT: To meet UL864 requirements for central station and remote station applications, set each day of the week to Yes for the required test report sked.
Reference
Schedules > Skeds > Sunday through Saturday

Xept on Holiday (Skeds)

Default: No
Selections: Yes/No
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.
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.
Reference
Schedules > Skeds > Xept on Holiday

Holiday 1 to Holiday 4

Default (Holiday 1 through Holiday 4): No
Selections: Yes/No
You can enable up to four holiday indexes to use with User Group Windows.
Enable at least one holiday index if Xept Holiday is set to Yes for this User Window, or if you want this window to activate only on specific dates.
Yes: Use the selected holiday index with this window.
No: Do not use the selected holiday index with this window.

Reference
Schedules > User Group Windows > Holiday 1 to Holiday 4 or
Schedules > Skeds > Holiday 1 to Holiday 4

12.4 Holiday Indexes

Holiday Indexes Schedule

This programming module is used to set holidays. Within each index, you can select up to 365 dates (or 366 dates for a Leap Year) to be designated as Holidays. Double-click in a cell corresponding to the Holiday Index you wish to program. The Holiday Schedule # dialog will appear. This dialog is formatted to look like a calendar. It opens to the current month and year.
The year is for reference purposes only. RPS only sends the month and day information to the Panel. When a day is chosen to be a holiday in a specific year that same day will be a holiday in every year thereafter. However, the day of the week will shift according to the year being viewed. For example if October 24, 2010, is set as a holiday, October 24 will be a holiday in 2011, 2012, and so on. But the holiday will fall on different days of the week.
Follow these steps to set a Holiday:

1. Double-click in a cell corresponding to the Holiday Index you wish to program. The Holiday Schedule # dialog will appear.
2. Double-click on the day of the holiday you wish to enable. Its box will turn red. If the month containing the Holiday you wish to program is not displayed, click on << Previous Month or Next Month >> until it is visible.
3. When you are finished setting your Holidays, click on OK. Click on Cancel to exit this dialog without saving any changes.

13 Access Control

13.1 Door, Strike, and Event Profiles

Door, Strike, and Event Profiles — Overview

Door Profile
This programming category is used to:
- Assign an area which also activates the D9210C
- Assign a point to the door
- Program the door state to change when the arm state changes
- Allow for the strike output to activate upon a fire alarm

Strike Profile
This programming category is used to create a specific door profile on:
- Strike and shunt times.
- Extending strike and shunt times if a door is left open.
- Resetting the strike when the door opens.
- Programming the interlock point.

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

Entry Area

Default: Disabled
Selections: 1 - 32
Assign an area to the door controller. This entry allows the D9210C to be polled, activating communication to the control panel. This also is the area a user will exit when initiating a request to exit (REX).

IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- All SDI devices, regardless of area assigned, will report to Area 1, Account 1 by default upon SDI failure. If a D9210C becomes disconnected, an SDI Fail ## and a MISSING POINT ### event will be created.
- [9210 NOT READY] will appear at this keypad when you press the ENTER key if the D9210B is not programmed with a *D# Entry Area*.

1 - 32: The area assigned to the door controller to which the reader will allow access.
Disabled: Door controller will not function.
Reference
Access Control > Door, Strike, and Event Profiles > Entry Area

Associated Keypad #

Default: 1
Selections: 1 - 16
This parameter sets the door controller to SDI2keypad associated for KP# Dual Authentication. A Setting of Disabled also disables Dual Authentication operation. Enter the Keypad number (KP#) 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.
1 - 16: This ***KP# Scope*** determines disarming rights. The user's access level in conjunction with the KP # Scope based on this keypad's scope and the user's Authority level.
Disabled: Only the area assigned to the D# Entry Area disarms for this door.
Reference
Access Control > Door, Strike, and Event Profiles > Associated Keypad #

Custom Function

Default: Disabled
Selections:
- D9412GV4: Disabled, CF 128 to CF 143
- D7412GV4: Disabled, CF 128 to CF 131

IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.

Use this parameter to program a custom function that activates at the keypad programmed for Scope.
This custom function only activates for users with a Function Level assignment that allows a valid ID to perform a custom function during the armed or disarmed state. The user to which the card or token is assigned must have an assigned passcode.
The following table shows how this programming affects custom function activation:

Function Level	Custom Function Activation
M (Armed)	User token activates the custom function assigned to the door controller only when the entry area for the door controller is All On or Part On.
D (Disarmed)	User token activates the custom function assigned to the door controller only when the entry area for the door controller is disarmed.
C (Armed and Disarmed)	User token activates the custom function assigned to the door controller only when the entry area for the door controller regardless of the armed state of the entry area.
Blank	User token does not activate the custom function assigned to the door controller.

Disabled: Custom function is disabled.
CF 128 to CF 143: The custom function number that activates when a valid ID is entered, given the appropriate user access level and area arm state.

Reference
Access Control > Door, Strike, and Event Profiles > Custom Function #

Door Point

Default: 0
Selections:
– **D9412GV4:** 0, 1 - 127, 129 - 247
– **D7412GV4:** 0, 1 - 75
Enter the point number that will be assigned to this door. This point cannot be used for any other point assignments.
Door Points must be programmed as Part On points. If a 24 hour point type is required for the Door Point, you may use a Part On point Type with a Point Response of 9 - C. Also, the Debounce Count must be set to 4 in Point Assignments.

IMPORTANT:
– This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
– Door points must be programmed as Part On points. If a 24-hour point type is required for the door point, you can use a Part On point type with a point response of 9 to C. Also, the debounce count must be set to 4 in Point Assignments.
– When assigning points 1-8 (panel zones), the end-of-line resistors must be removed from the panel. In addition to this, do not enable any POPIT points (or OctoPOPIT points) sharing the same point number as the Door Point. Failure to do so will result in Extra Point trouble conditions upon reboot.

1 - 127, 129 - 247: The point number assigned to this door. Points 128 and 248 are reserved by the panel for internal use.
0: There is no point number assigned to this door.

RPS Menu Location
Access Control > Door, Strike, and Event Profiles > Door Point

Interlock Point

Default: 0
Selections:
– **D9412GV4:** 0, 1 - 127, 129 - 247
– **D7412GV4:** 0, 1 - 75
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 door point. You may assign it to another controller, thereby having one interlock point prevent multiple controllers from activating.

IMPORTANT:
– This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
– Door points must be programmed as Part On points. If a 24-hour point type is required for the door point, you can use a Part On point type with a point response of 9 to C. Also, the debounce count must be set to 4 in Point Assignments.

CAUTION: The interlock point will be considered in a normal state if it is bypassed, swinger bypassed, or forced armed. This will result in normal operation of access even if the door is left open.

1 - 127, 129 - 247: The point number assigned to the interlock point. Points 128 and 248 are reserved by the panel for internal use.
0: There is no point number assigned to the interlock point.

RPS Menu Location
Access Control > Door, Strike, and Event Profiles > Interlock Point

13.1.1 Auto Door

Default: No
Selections: Yes or No
Use this program item to unlock the door (latched shunt and strike) automatically when the entry area is disarmed. The door will re-lock upon All On or Part On arming the area.

IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- The Unlocked state cannot be overridden manually.

Yes: When the area assigned in D# Entry Area is disarmed, the door will be in the Unlocked state. When that area is armed, the door will return to the Locked state.
No: Door state will not be affected by the armed state of the area.
RPS Menu Location
Access Control > Door, Strike, and Event Profiles > Auto Door

Fire Unlock

Default: No
Selections: Yes or No
Use this program item to activate the output for the door strike and shunt the door zone automatically upon a Fire or Gas Alarm. This feature will override a Secure Door state, Locked Door state, Auto Door, and an Interlock faulted point. The output activates for all doors with this prompt programmed YES when a Fire or Gas Alarm occurs in any area. Outputs that are activated by Fire Unlock can only be returned to normal through the keypad using [MENU 38] (Door Control) on the keypad.

IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- This will unlock the door regardless of the armed state.
- Doors that are activated by Fire Unlock must be returned to normal using [MENU 38] (Door Control) on the keypad.
- Bosch Security Systems does not recommend use of the Fire Unlock feature on door controllers intended to be used for Dual Authentication because it will prevent execution of the configured Passcode Function.

Yes: Output will activate and shunt will be applied for the door contact automatically upon a Fire or Gas Alarm.
No: Door will remain in its current mode upon a Fire or Gas Alarm.
Reference
Access Control > Door, Strike, and Event Profiles > Fire Unlock

Disarm On Open

Default: Yes
Selections: Yes or No
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
Use this program item to determine whether the door needs to be physically opened prior to disarming the area upon a valid access request. The user initiating the access request must have access levels that allow disarming with ID.
Yes: The area will disarm only after the door has been opened for an access user with disarm authority.
No: The area will disarm whether or not the door has been opened as soon as a user with a valid disarm level has presented a valid token/card.
Reference
Access Control > Door, Strike, and Event Profiles > Disarm On Open

Card Type

Default: 26 bit
Selections:
– 26 bit
– 37 bit
This parameter specifies the card format used for all of the door controllers.
26 bit: Site Code will be set to 255.
37 bit: Site Code will be set to 0.
IMPORTANT
Changing this parameter erases all entries currently under Card Data, and Site Code fields returns to factory defaults.
Reference
Access Control > Door, Strike, and Event Profiles > Card Type

Strike Time

Default: 10
Selections: 1 - 240 seconds
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
Enter the amount of time the output for the strike will activate to allow a user to open the door. The strike will activate upon a valid token, Request to Enter (RTE), Request to Exit (REX), and the keypad [CYCLE DOOR?] function.
Blank: Strike Time is not programmed for this door.
1 - 240: The strike will activate for the amount of time programmed.
Reference
Access Control > Door, Strike, and Event Profiles > Strike Time

Shunt Time

Default: 10
Selections: Blank, 1 - 240 seconds
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
Enter the amount of time that the door point will be shunted to allow a user to open the door without causing the point to go into Trouble, Alarm, or a faulted condition.

Blank: Shunt Time is not programmed for this door.
1 - 240: The shunt will activate for the amount of time programmed.
Reference
Access Control > Door, Strike, and Event Profiles > Shunt Time

Buzz Time

Default: 2
Selections: Blank, 1 - 240 seconds
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
Enter the amount of time that the buzzer output will activate to notify the user that the strike has been activated and the door is ready to open. The buzzer will stop as soon as the door is opened.
A separate buzzer is required. Many readers have an internal buzzer that is not affected by Buzz Time.
Blank: Buzz Time is not programmed for this door.
1 - 240: The buzzer will sound for the amount of time programmed.
Reference
Access Control > Door, Strike, and Event Profiles > Buzz Time

Extend Time

Default: 10
Selections: Blank, 1 - 30 Seconds
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
Enter the amount of time that strike, buzz, and shunt activation will be prolonged if a door is left open and the shunt time expires. At the end of the programmed extend time, the buzzer will continue to buzz until the door is closed. In addition, if programmed, the point assigned to the door will indicate a Trouble, Alarm, or Fault at the keypad.
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 has returned to normal.
Reference
Access Control > Door, Strike, and Event Profiles > Extend Time

Deactivate On Open

Default: Yes
Selections: Yes or No
This program item determines whether the strike will deactivate immediately upon physically opening the door.
In order for this function to work, a point needs to be assigned to the door.
IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- To reduce false alarms, leave this programming item at YES (default). This will help prevent the door from "bouncing" open and causing a false alarm.

Yes: Strike will deactivate when the door is opened after a valid access granted request.
No: Strike will remain activated for the amount of the programmed strike time whether door is opened or closed.
Reference
Access Control > Door, Strike, and Event Profiles > Deactivate On Open

RTE Shunt Only

Default: No
Selections: Yes or No
Use this program item to disable the strike, but still activate the programmed shunt time upon a *Request to Enter* an area.
Use this parameter when a user can open a door manually without relying on a token/card to activate the strike (such as with a "push bar").
IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- When RTEShunt Only is "Yes," Request To Enter events are not logged or reported.

Yes: Programmed shunt time will activate so door can be manually opened.
No: Request to Enter (RTE) automatically activates the programmed strike and shunt time.
Reference
Access Control > Door, Strike, and Event Profiles > RTE Shunt Only

REX Shunt Only

Default: No
Selections: Yes or No
Use this program item to disable the strike, but still activate the programmed shunt time upon a *Request to Exit* an area.
Use this parameter when a user can open a door manually without relying on a token/card to activate the strike (such as with a "push bar").
IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- When REXShunt Only is "Yes," Request To Exit events are not logged or reported.

Yes: Programmed shunt time will activate so door can be manually opened.
No: Request to Exit (REX) automatically activates the programmed strike and shunt time.
Reference
Access Control > Door, Strike, and Event Profiles > REX Shunt Only

13.1.2 Access Granted

Default: Yes
Selections: Yes or No
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
This program item determines if ACCESS GRANTED and DOOR REQUEST events are sent to the control panel to be entered in the event log, and remote reporting.
A successful access event can be initiated by:
– a valid user ID
– a valid door state changed at the keypad
– an automatically scheduled or armed state changes that hold a door open
– a request to enter/exit (RTE/REX).
Yes: Access events from this door controller will be sent to the control panel for processing.
No: Access events from this door controller will not be sent to the control panel for processing.
Reference
Access Control > Door, Strike, and Event Profiles > Access Granted

No Entry

Default: Yes
Selections: Yes or No
IMPORTANT: This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
This program item determines if `No Entry` events are sent to the control panel to be entered in the event log, and remote reporting.
A No Entry event may be caused by:
– invalid or unknown user ID, interlock or secured door, or incorrect authority level
– request to enter/exit (RTE/REX) for door in interlock or secured door
Yes: Access denied events from this door controller will be sent to the control panel for processing.
No: Access denied events from this door controller will not be sent to the control panel for processing.
Reference
Access Control > Door, Strike, and Event Profiles > No Entry

Enter Request

Default: No
Selections: Yes or No
This program item determines if Request to Enter (RTE) events are sent to the control panel to be entered in the event log, and remote reporting.
IMPORTANT:
– This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
– RTE events require D# Access Granted to be programmed YES.
Yes: A `DOOR REQUEST TO ENTER` event from this door controller is sent to the control panel for processing.
No: A `DOOR REQUEST TO ENTER` event from this door controller is not sent to the control panel for processing.

Reference
Access Control > Door, Strike, and Event Profiles > Enter Request

Exit Request

Default: No
Selections: Yes or No
This program item determines if Request to Exit (REX) events are sent to the control panel to be entered in the event log, and remote reporting.

IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- REX events require D# Access Granted to be programmed YES.

Yes: A `DOOR REQUEST TO EXIT` event from this door controller is sent to the control panel for processing.
No: A `DOOR REQUEST TO EXIT` event from this door controller is not sent to the control panel for processing.
Reference
Access Control > Door, Strike, and Event Profiles > Exit Request

Door Descriptions

Default:
- **Door 1:** DOOR 1
- Door 2: DOOR 2
- Door 3: DOOR 3
- Door 4: DOOR 4
- Door 5: DOOR 5
- Door 6: DOOR 6
- Door 7: DOOR 7
- Door 8: DOOR 8

Selections: Up to 24 Characters Alphanumeric

IMPORTANT:
- This parameter is available only in the D9412GV4 and D7412GV4 control panel accounts.
- The D9412GV4 supports Doors 1-8. The D7412GV4 supports Doors 1 and 2.

Enter up to 24 characters of text to describe the door.
This is for informational purposes only and is not programmed in the control panel.
Reference
Access Control > Door Profile > Door Descriptions

14 Automation

Automation Device

Default: None
Selections:
None,
SDI address 80,
Mode 1 SDI address 80,
Mode 1 SDI2 address 1,
Mode 1 SDI2 address 2,
Mode 2
This prompt enables and selects the communication module to use exclusively for automation communication.
Select SDI address 80 to enable the automation address (SDI Address 80) for the DX4010V2 or DX4010i Serial Interface Module, or DX4020 Network Interface Module.
Select SDI2 address 1 to enable automation using a B426 (B420) Ethernet Communication Module at address 1 on the SDI2 bus.
Select SDI2 address 2 to enable automation using a B426 (B420) Ethernet Communication Module at address 2 on the SDI2 bus
RPS Menu Location
Automation > Automation Device

Enable SDI Address 80 supervision

Default: No
Selections: Yes or No
Select **Yes** to enable supervision of the automation devices at SDI address 80 for the DX4010V2 or DX4010i Serial Interface Module, or DX4020 Network Interface Module.
NOTE: This parameter is only applicable when the Automation Device is set to **SDI address 80**. The automation devices on the SDI2 bus will always be supervised.
RPS Menu Location
Automation > Enable SDI Address 80 Supervision

Status Rate

Default: 0
Selections: 0 - 255
This item determines how often the default status information is sent to the DX4020, DX4010V2, DX4010i, or D9133 Serial Interface Module. The Status information includes the current point status (normal or off-normal), the control panel's area status (All On, All On Instant, Part On Delay Armed, Part On Instant Armed, Disarmed, Area Entry Delay, Part On Entry Delay, Area Exit Delay, Part On Exit Delay), the control panel status (AC fail, battery missing, AC restore, battery low, and so on), and output status (output on or output off).
Entries are in 100 millisecond increments. Therefore, if a 5 is entered, the Status information is sent every 500 milliseconds (or ½ second). An entry of 10 would equal 1 second.
IMPORTANT: If the Status Rate is set to a value under 10 and there are 1 – 6 SDI devices connected to the system, the fastest the control panel can send the Status information is

approximately 1 second. In addition to this, if there are more than 6 SDI Devices connected to the control panel, the fastest the control panel can send the information is approximately 1½ to 2 seconds.

0: Status information never sent *unless requested*.

1 – 255: Status information is sent at the interval programmed.

RPS Menu Location

Automation > Status Rate

Automation Passcode

Default: Bosch_Auto

Selections:

- Valid characters: A-Z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

This parameter sets the passcode that must be entered before automation software can connect to the control panel.

This parameter accepts up to 24 characters, but allows shorter passcodes. The minimum length is six characters. The standard ASCII character set except space is supported. The passcode is case-sensitive. The automation passcode must be entered before any other automation commands will be accepted by the control panel.

RPS Menu Location

Automation > Automation Passcode

Application Passcode

Default: Bosch_RSC

Selections:

- Valid characters: A-Z, a-z, 0-9, ?, &, @, -, *, +, $, #, _, /
- Invalid characters: Period (.) comma (,) percent (%), parenthesis [()], equal (=), greater/less than (<>), exclamation (!), braces ({}), apostrophe ('), carat (^), grave accent (`), tilde (~), semi-colon (;), colon (:), brackets ([]), forward slash (\), vertical bar (|)

This parameter sets the passcode that must be entered before application software can connect to the control panel.

This parameter accepts up to 24 characters, but allows shorter passcodes. The minimum length is six characters. The standard ASCII character set except space is supported. The passcode is case-sensitive. The application passcode must be entered before any other application commands will be accepted by the control panel.

RPS Menu Location

Automation > Application Passcode

15 SDI2 Modules

15.1 B208 Octo-input

B208 Octo-input Information

The B208 Octo-input is an device that attaches to the SDI2 bus of the GV4 control panel. Each module provides 8 independently monitored control loops.

Capacity

Panel type	Modules supported
D9412GV4	24
D7412GV4	7

Settings

RPS supports the configuration of the Enclosure Tamper on each of the Octo-input modules. **Yes** = Enable enclosure tamper, **No** = Disable enclosure tamper. Default setting is No.

Switch Settings

Ref. Hardware Switch Settings > SDI2 Devices > B208 Octo-input Switch Settings

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.

RPS Menu Location

SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

15.2 B308 Octo-output

B308 Octo-output Information

The B308 Octo-output is a device that attaches to the SDI2 bus of the GV4 control panel. It provides 8 independently controlled outputs similar in function to those provided by the Zonex output modules.

Capacity

Panel type	Modules supported
D9412GV4	12
D7412GV4	6

Settings

RPS shall support the configuration of the Enclosure Tamper on each of the Octo-output modules. **Yes** = Enable enclosure tamper, **No** = Disable enclosure tamper. Default setting is No.

Switch Settings

Reference Hardware Switch Settings > SDI2 Devices > B308 Octo-output Switch Settings

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.

RPS Menu Location
SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

15.3 IP Communicator

IP Communicator Overview

The B426 (B420) Ethernet Communication Module (NIM) 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, 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.

Capacity

Panel type	Modules supported
D9412GV4	2
D7412GV4	2

You can use one or both communication modules for central station reporting or RPS communications. Optionally, you can use one of the B426 (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.

IMPORTANT:

- To prevent communication loss, the configuration sent to the control panel for the B426 (B420) module takes effect after RPS disconnects from the control panel.
- If the B426 (B420) is configured through the B426 (B420) configuration web interface to disable control panel programming (that is, **Panel Programming Enable** is set to No), then RPS programming of the B426 (B420) is accepted by the control panel, but not applied to the B426 (B420). The **Panel Programming Enable** parameter is not available in RPS.

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.
RPS Menu Location
SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

IPv6 Mode

Default: No
Selections:
– Yes = IPv6 enabled
– No = IPv6 disabled
Yes When using a B426 module, set IPv6 Mode to Yes.
No When using a B420 module, set IPv6 Mode to No.
This parameter controls which configuration items are available based on the mode being used.
A B426 module is required for IPv6 communications.
1 When IPv6 mode is set to Yes and a B420 is actually connected, one of the two following situations occurs:
When a B420 is connected, the control panel configures the B420 based on the settings provided by RPS, even if RPS enabled IPv6 mode. DHCP must be set to yes, for IPv4 communications to work correctly. An attempt to communicate with an IPv6 only address would fail. Attempting to report to an IPv6 only address results in a Comm Trouble.
2 The control panel recognizes that IPv6 mode has been selected and that a B420 has been connected. Since the B420 does not support IPv6 mode, an Invalid Module system fault is created.

When IPV6 Mode is enabled, then RPS makes the following parameters Read Only:
– IPv4 Address
– IPv4 Subnet Mask
– IPv4 Default Gateway
– IPv4 DNS Server IP Address

When IPv6 Mode is disabled, then RPS makes the following parameters Read Only:
– IPv6 Address
– IPv6 Subnet Prefix Length
– IPv6 Default Gateway
– IPv6 DNS Server IP Address
RPS Menu Location
SDI2 Modules > IP Communicator > IPv6 Mode

IPv4 DHCP/AutoIP Enable

Default: Yes
Selections: Yes/No
This parameter configures the on-board Ethernet communicator automatically using DHCP (Dynamic Host Configuration Protocol).
Yes DHCP automatically configures the module's IPV4 Address, IPV4 Default Gateway, and IPV4 DNS Server Address. These parameters are grayed out and you cannot edit them manually.
No DHCP is disabled. You must manually configure the B426 (B420).
AutoIP enables dynamic IP addresses to be assigned to a device when the device is started up. A host configured with AutoIP receives an IP address of 169.254.xxx.xxx. Whereas DHCP requires a DHCP server, AutoIP does not require a server when selecting an IP address.
If you set IPv6 Mode to Yes, set DHCP/AutoIP Enable to Yes.
The parameter has no effect on B450 operation.

RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 DHCP/AutoIP Enable.

IPv4 Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter sets the IPv4 address for the indicated On-board Ethernet Communicator. This is the IPv4 address for the indicated B426 (B420) Ethernet Communication Module. When this is defined through the DHCP service, leave the default value.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 address.

IPv4 Subnet Mask

Default: 255.255.255.255
Selections: 0.0.0.0 to 255.255.255.255
The IPv4 Sub-network Mask has a dot decimal notation, which consists of the four octets of the address expressed separately in decimal and separated by periods. Each octet has a value 0-255.
When this is defined through the DHCP service, leave the default value.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 subnet mask.

IPv4 Default Gateway

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter configures the IPv4 Default Gateway.
The IPv4 Gateway (or node) address has a dot decimal notation, which consists of the four octets of the address expressed separately in decimal and separated by periods. Each octet has a value 0-255. This is the address of the local network gateway to the Internet or Intranet.
When this is defined through the DHCP service, leave the default value.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 default gateway.

IPv4 DNS Server IP Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter configures the IPv4 DNS server address in Static IP mode.
The IPv4 Domain Name Server (DNS) address has a dot decimal notation, which consists of the four octets of the address expressed separately in decimal and separated by periods. Each octet has a value 0-255.
When this is defined through the DHCP service, leave the default value.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 DNS server IP address.

IPv6 DNS Server IP Address

Default: ::
Selections: 0000:0000:0000:0000:0000:0000:0000:0000 to FFFF:FFFF:FFF:FFFF:FFFF:FFFF:FFFF:FFFF
This parameter configures the IPv6 DNS server address in Static IP mode.
A Domain Name Server (DNS) converts internet domain names or host names to their corresponding IP addresses. In DHCP mode, the default value indicates the DHCP server's default DNS will be used. To use a custom DNS server in DHCP mode, change the parameter to the specified DNS server's IP address.
The IPv6 Domain Name Server (DNS) address has a hexadecimal notation, which consists of the eight groups of the address expressed separately in hexadecimal and separated by colons. Each group can have a value between 0000-FFFF.
When this is defined through the DHCP service, leave the default value.
For IPv6, only the DNS server addresses are entered as numbers. All other entries should be limited to IPv4 addresses or DNS names.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv6 DNS Server IP Address

UPnP (Universal Plug and Play) Enable

Default: No
Selections: Yes/No
Yes Enables IP devices to discover each other's presence on the network and establish functional network services for communications. A Yes setting also allows a router to forward port numbers through itself, allowing reports to reach receivers behind the router.
No UPnP is disabled.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > UPnP (Universal Plug and Play) Enable

HTTP Port Number

Default: 80
Selections: 1 to 65535
The default Hypertext Transfer Protocol (HTTP) port is typically 80.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > HTTP Port Number.

ARP Cache Timeout

Default: 600
Selections: 0 to 600 (seconds)
This specifies the time-out for ARP cache entries (time-out value in seconds).
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > ARP cache timeout.

Web/USB Access Enable

Default: Yes
Selections: Yes/No
Yes Web access enabled.
No Web access disabled.
This parameter allows authorized users to view and modify configuration parameters for the B426 (B420) through a standard web browser.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > Web/USB Access Enable.

Web/USB Access Password

Default: ****** (B42V2)
Selections: 4 to 10 characters in length.
This parameter sets the password for web access.
After you set the password, RPS will not show the characters when you enter the password in the future. A “space” string disables the password check.
Reference
SDI2 Modules > IP Communicator > Web/USB Access Password.

Firmware Upgrade Enable

Default: No
Selections: Yes/No
Yes Firmware Upgrade enabled.
No Firmware Upgrade disabled.
This parameter enables the B426 (B420)’s firmware to be modified via the external Web interface, not by the control panel.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > Firmware Upgrade Enable.

Module Hostname

Default: Blank
Selections: Up to sixty-three characters (Letters, Numbers, and Dashes)
Use this parameter to create a module hostname name. This is the hostname that represents the communication device 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 hostname for the purposes of configuration and diagnostics.
Input characters are restricted by the RFC 1123 Requirements for Internet Hosts -- Application and Support. Note: Setting the hostname to a blank will cause the Ethernet communicator module to return to its factory default hostname.
The parameter has no effect on B450 operation.
Reference
SDI2 Modules > IP Communicatore > Module Hostname.

Unit Description

Default: Blank
Selections: Up to twenty alphanumeric characters.
This field describes the B426 (B420) module (location, attributes, etc.). 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.
The parameter has no effect on B450 operation.
Reference
SDI2 Modules > IP Communicator > Unit Description.

TCP/UDP Port Number

Default: 7700
Selections: 0 - 65535
This parameter sets the local port number that the module listens to for in-coming network traffic.
The TCP/UDP Port option is used for the B426 (B420) to communicate with GV4 Series control panels for RPS or other outside connections.
Port numbers are assigned in various ways based on three ranges:
System Ports 0-1023
User Ports 1024-49151
Dynamic or Private Ports 49152-65535
Note: In order to limit unwanted traffic, select a number above 1023.
Reference
SDI2 Modules > IP Communicator > TCP/UDP Port Number.

TCP Keepalive Time

Default: 45
Selections: 0 - 65 (seconds)
The time in seconds between TCP keep-alive transmissions to verify that an idle connection is still active.
The parameter has no effect on B450 operation.
Reference
SDI2 Modules > IP Communicator > TCP Keepalive Time.

IPv4 Test Address

Default: 8.8.8.8
Selections: IPv4 address or Domain Name
Input characters are according to RFC 1123 Requirements for Internet Hosts -- Application and Support. The IPv4 Test Address is used by the B426 (B420) to ping an internet address as part of the IP diagnostics.
Reference: Allowable formats for the IPv4 Test Address... Network Address Format
RPS Menu Location
SDI2 Modules > IP Communicator > IPv4 Test Address.

IPv6 Test Address

Default: 2001:4860:4860::8888
Selections: IPv6 address or Domain Name
This parameter sets the IPv6 Test Address. The IPv6 Test Address is used by the On-board IP connection to ping an internet address in order to verify the integrity of the network and the network configuration setting. This parameter is only available when IPv6 Mode is set to Yes.
RPS Menu Location
SDI2 Modules > IP Communicator > IPv6 Test Address.
Additional Resources:
Network Address Format

Web and Automation Security

Default: Enable
Selections: Disable, Enable
This parameter enables enhanced security for Automation and B426 Web Access.
Disable Enhanced security is not applied.
Enable Enhanced security is applied.
When enabled, HTTPS is applied to B426 Web Access changing the default value of the HTTP Port Number parameter. This setting also enables TLS Security for Automation.
Reference
SDI2 Modules > IP Communicator > Web and Automation Security

Alternate IPv4 DNS server IP address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter provides and alternate IPv4 DNS server IP address.
If the module fails to obtain an address from the primary server, the alternate DNS server will be used if one has been specified. Use the same rules as the DNS server address. When this is defined through the DHCP service, leave the default value.
RPS Menu Location
SDI2 > IP Communicator > Alternate IPv4 DNS server IP address

Alternate IPv6 DNS server IP address

Default: ::
Selections: 0000:0000:0000:0000:0000:0000:0000:0000 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
This parameter provides and alternate IPv6 DNS server IP address.
If the module fails to obtain an address from the primary server, the alternate DNS server will be used if one has been specified. Use the same rules as the DNS server address. When this is defined through the DHCP service, leave the default value.
RPS Menu Location
SDI2 Modules > IP Communicator > Alternate IPv6 DNS server IP address.

15.3.1 B450 Cellular

Inbound SMS

Default: Yes
Selections:
Yes Enable downloads.
No Disable downloads.
This parameter enables an RPS user to start a control panel initiated download with an SMS message.
RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inbound SMS

Session Keep Alive Period

Default: 0
Selections: 0 to 1000 min
0 Disabled. Panel does not verify the connection is active.
1-1000 Enabled. Panel verifies an active connection exists.
This parameter sets the length of time in minutes between session keep alive reports to verify that an idle connection is still active. Leave the default value.
RPS Menu Locations
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Session Keep Alive Period

Inactivity Timeout

Default: 0
Selections: 0 to 1000 min
0 Disabled. Panel does not verify the connection is active.
1-1000 Enabled. Panel verifies an active connection exists.
This parameter specifies the time before the control panel will disconnect a session with no data traffic. Leave the default value.
RPS Menu Selection
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inactivity Timeout

Reporting Delay for Low Signal Strength

Default: 1800
Selections: 0-3600 (seconds)
0 Disabled.
1-3600 The amount of time needed to determine low signal strength.
IMPORTANT To meet UL requirements, the entry for this parameter should not exceed 200 seconds.
This parameter sets the amount of time needed to determine the signal strength is low.
The B440 module indicates if its cellular signal strength is low only if the configuration item for Reporting Delay for Low Signal Strength is set to a value other than zero, and the signal strength is below a pre-determined "unacceptable"

threshold (indicated by the red LED) for 80% of the measurements taken during the most recent time period specified by that configuration parameter.
This event is restored by the signal being above the "good" threshold (indicated by the green LED) for 80% of the measurements during the same configuration parameter. The control panel logs a Cellular Low Signal event upon detecting this event, and Cellular Low Signal Restoral event upon restoral.

Cellular Settings for High Supervision Sites (Faster than 1 hour supervision)
The vast majority of cellular installations can be supervised at settings of 4 hours to 25 hours, but for high security and fire listed installations where cellular is the primary or sole communication path and supervision rates are 1 hour or less you should consider changing the following cellular parameters in the panel or cellular device bus module:

1 **Reporting Delay for Low Signal & Reporting Delay for No Towers:** 200 seconds. For some listed high security installations, low cellular signal is required be treated like a wire cut and reported within 200 seconds. This will increase sensitivity to cellular tower maintenance windows and other environmental conditions, so we recommend leaving the default settings for non-listed installations.

2 **Reporting Delay for Single Tower**: 600 seconds. For sole path cellular sites with supervision at 5 minutes or less where only one cell tower is available, maintenance (generally 1-5 minutes in the early morning hours) or changes in environmental conditions may cause communication troubles to be reported. To detect and report single tower conditions at cellular sites using a plug-in cellular module in the panel or on GV4 version 2+ or B Series SDI2 bus, enable Single Tower trouble reporting. The number of towers available can be viewed in the B450 module's USB menu or on keypads of SDI2 control panels with version 2+.

NOTICE: For SDI and Option bus installations of a cellular module, trouble conditions such as Low Signal and Single Tower result in the device going missing from the bus when the delay timer is reached.

RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Low Signal Strength

Reporting Delay for No Towers

Default: 1800
Selections: 0-3600 (seconds)

0 Disabled.

1-3600 Enabled. The amount of time in seconds needed to determine no tower is available.

This parameter allows the control panel to indicate if there is no tower available for communication if the event has been present for the duration specified here.
This event is restored by one or more towers becoming available for the duration specified by that parameter. The control panel logs an event upon detecting this event, and upon restoral.

Cellular Settings for High Supervision Sites (Faster than 1 hour supervision)
The vast majority of cellular installations can be supervised at settings of 4 hours to 25 hours, but for high security and fire listed installations where cellular is the primary or sole communication path and supervision rates are 1 hour or less you

should consider changing the following cellular parameters in the panel or cellular device bus module:

1 **Reporting Delay for Low Signal & Reporting Delay for No Towers:** 200 seconds. For some listed high security installations, low cellular signal is required be treated like a wire cut and reported within 200 seconds. This will increase sensitivity to cellular tower maintenance windows and other environmental conditions, so we recommend leaving the default settings for non-listed installations.

2 **Reporting Delay for Single Tower**: 600 seconds. For sole path cellular sites with supervision at 5 minutes or less where only one cell tower is available, maintenance (generally 1-5 minutes in the early morning hours) or changes in environmental conditions may cause communication troubles to be reported. To detect and report single tower conditions at cellular sites using a plug-in cellular module in the panel or on GV4 version 2+ or B Series SDI2 bus, enable Single Tower trouble reporting. The number of towers available can be viewed in the B450 module's USB menu or on keypads of SDI2 control panels with version 2+.

NOTICE: For SDI and Option bus installations of a cellular module, trouble conditions such as Low Signal and Single Tower result in the device going missing from the bus when the delay timer is reached.

RPS Menu Locations
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for No Towers

Reporting Delay for Single Tower

Default: 0
Selections: 0-3600 (seconds)

0 Disabled.

1-3600 Enabled. The amount of time in seconds needed to determine only one tower is available.

This parameter allows the control panel to indicate if there is only one tower available for communication if the event has been present for the duration specified here. This event is restored by two or more towers becoming available for the duration specified by that parameter. The control panel logs an event upon detecting this event, and upon restoral.

Cellular Settings for High Supervision Sites (Faster than 1 hour supervision)
The vast majority of cellular installations can be supervised at settings of 4 hours to 25 hours, but for high security and fire listed installations where cellular is the primary or sole communication path and supervision rates are 1 hour or less you should consider changing the following cellular parameters in the panel or cellular device bus module:

1 **Reporting Delay for Low Signal & Reporting Delay for No Towers:** 200 seconds. For some listed high security installations, low cellular signal is required be treated like a wire cut and reported within 200 seconds. This will increase sensitivity to cellular tower maintenance windows and other environmental conditions, so we recommend leaving the default settings for non-listed installations.

2 **Reporting Delay for Single Tower**: 600 seconds. For sole path cellular sites with supervision at 5 minutes or less where only one cell tower is available, maintenance (generally 1-5 minutes in the early morning hours) or changes in environmental conditions may cause communication troubles to be reported. To detect and report single tower conditions at cellular sites using a plug-in cellular module in the panel or on GV4 version 2+ or B Series SDI2 bus, enable Single Tower trouble reporting. The number of towers available can be viewed in the B450 module's USB menu or on keypads of SDI2 control panels with version 2+.

NOTICE: For SDI and Option bus installations of a cellular module, trouble conditions such as Low Signal and Single Tower result in the device going missing from the bus when the delay timer is reached.

RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Single Tower

Outgoing SMS Length

Default: 160
Selections: 0 to 3600 characters

0 Disabled. The control panel does not verify the connection is active.

1-3600 Enabled. The control panel verifies an active connection exists.

This parameter sets the acceptable length for outgoing messages.
Outgoing SMS messages are truncated if over this length. This must match the cellular network that is transmitting the SMS message (i.e.: Verizon).
RPS Menu Locations
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Outgoing SMS Length

Cellular SIM Card Parameters

SIM PIN

Default: Blank
Selections: 4-8 numbers
This is an optional parameter. This parameter is only necessary if the SIM card uses a PIN for security.
The SIM PIN is hidden on the display and appears as asterisks (********) when entered. If an invalid SIM PIN is entered, an event is logged in history. A report is sent only if the report function is enabled. If no SIM PIN is required, you can leave the field blank.
RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > SIM PIN

Network Access Point Name

Default: gne.apn
Selections: 0-99 ASCII characters
This parameter sets the IP address for the network access point.
Enter up to 99 alphanumeric characters. The field is case sensitive.

RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point Name

Network Access Point User Name

Default: Blank
Selections: 0-30 ASCII characters
This parameter specifies the user name for the Network Access Point.
Enter up to 30 alphanumeric characters. The field is case sensitive.
RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point User Name

Network Access Point Password

Default: Blank
Selections: 0-30 ASCII characters
This parameter sets the password required to access the Network Access Point.
Enter up to 30 alpha-numeric characters. The password is case sensitive.
RPS Menu Location
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point Password

15.4 B520 Aux Power Supply

B520 Aux Power Supply Information

The B520 Auxiliary Power Supply is an device that attaches to the SDI2 bus of the GV4 control panel. It provides a supervised 12 Volt DC 2.5 Amp auxiliary power supply. Each power supply may support 2 separate 12V nominal lead acid batteries with a capacity of 7-18 Ah.

Capacity

Panel type	Modules supported
D9412GV4	8
D7412GV4	8

Additional Information
B520 Power Supply Switch Settings

Module Enable

Default: No
Selections: Yes or No
Module Enable indicates to the panel if the SDI2 module should be supervised.
RPS Menu Location
SDI2 Modules > B520 Aux Power Supply > B520 Module Enable

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.
RPS Menu Location
SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

One or Two batteries

Default: One
Selections: One or Two
This parameter will notify the panel if 1 or 2 backup batteries are installed with the Auxiliary Power Supply module.
RPS Menu Location
SDI2 Modules > B520 Aux Power Supply > One or Two Batteries

15.5 Wireless Receiver

Wireless Receiver Information

The B820 SDI2 Inovonics Interface Module is supported on the SDI2 bus of the GV4 control panel. It provides an ability to use wireless keyfobs, Repeaters and Points with the GV4 control panel.
Capacity
The control panel supports two types of SDI2 wireless interface modules:
– B810 RADION Wireless
– B820 Inovonics Wireless
Only one wireless module can be used at a time and all points, repeaters and keyfobs must be of the same type.
IMPORTANT Choose the type of wireless module before any points, users or repeaters are added to the system. If you change wireless types will cause all RF information to reset to its factory defaults. All previously configured RF information will be lost and will need to be re-entered.
Additional Information
Wireless Receiver Switch Settings

Wireless Module Type

Default: B810 RADION Wireless
Selections:
- Unassigned
- B810 RADION Wireless
- B820 Inovonics Wireless

This prompt enable and selects the type of wireless receiver that will be used with the system.
If no wireless devices will be used, select Unassigned.
RPS Menu Location
SDI2 Modules > Wireless Receiver > Wireless Module Type

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.
RPS Menu Location
SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

System Supervision Time

Default: 12 Hours
Selections: None, 4, 12, 24, 48, 72 hours
None = no wireless device supervision, **4, 12, 24, 48, 72 hours** = hours between hearing from the Wireless receiver before sending a missing condition.
RPS supports the configuration of the global System Supervision Time for wireless repeaters configured to report to the wireless receiver. This value is used to set the supervision time for all repeaters configured to report to the wireless receiver. If a user is configured as supervised, the supervision time for that user is set to 4 hours. A point's supervision time is set in the point index field for that point. RADION keyfobs are not supervised when assigned to a User. RADION keyfobs will follow the supervision rules if configured as a point device.
All fire points are fixed at a 4 hour supervision time regardless of the System Supervision Time setting.
RPS Menu Location
SDI2 Modules > Wireless Receiver > System Supervision Time

Low Battery Resound

Default: Never Resound
Selections: Never Resound, 4, 24 hours
This setting is global for all non-fire points. The panel will automatically fix the Low Battery Resound at 24 hours for fire and gas points
RPS Menu Location
SDI2 Modules > Wireless Receiver > Low Battery Resound

Enable Jamming Detection

Default: Yes
Selections: Yes/No
This parameter setting turns on or off the reporting of interference to the control panel.
The B810 RADION Wireless module detects RF jamming (interference) when it is present. Jamming Detection can be disabled for the B810 RADION Wireless module. The B820 Inovonics Wireless module also detects RF jamming (interference) when it is present. Jamming Detection cannot be disabled for the B820 Inovonics Wireless module.
RPS Menu Location
SDI2 Modules > Wireless Receiver > Enable Jamming Detection

15.6 Wireless Repeater

Wireless Repeater Information

The Wireless Repeater modules are independent of the SDI2 bus. They provide the ability to extend the range of the B820 Inovonics SDI2 Wireless Interface Module for an installation site.
Capacity
The control panel supports two types of SDI2 wireless interface modules:
- B810 RADION Wireless
- B820 Inovonics Wireless

The type of wireless repeater must match the type of receiver. It is highly recommended that the type of wireless receiver is chosen before any repeaters are configured.
The control panel will support up to 8 repeaters simultaneously. All repeaters must be of the same type.
Settings
RPS supports the configuration of the Enclosure Tamper on each of the Wireless Repeater modules. **Yes** = Enable enclosure tamper, **No** = Disable enclosure tamper. Default setting is Yes.
RPS supports the configuration of the RFID for each of the Wireless Repeater modules.
There are no hardware switches on a Wireless Repeater. The Wireless Repeater number is determined by the location of the RFID within the configuration table.
Notes
Even though the Wireless Repeater 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.

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes: Indicates that the panel will monitor the tamper status of an SDI2 device and report its state changes accordingly.
No: The panel will ignore any tamper state changes being sent by an SDI2 device to the panel.
Use this parameter to set the Enclosure Tamper indication of a particular SDI2 device. When setting this parameter to Yes it typically indicates that the SDI2 device has a tamper switch that activates when the device enclosure is opened, or removed from its mounting location.
RPS Menu Location
SDI2 Modules > B208 Octo-input > Module Enclosure Tamper
SDI2 Modules > B308 Octo-output > Module Enclosure Tamper
SDI2 Modules > IP Communicator > Module Enclosure Tamper
SDI2 Modules > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 Modules > Wireless Receiver > Module Enclosure Tamper
SDI2 Modules > Wireless Repeater > Module Enclosure Tamper

RFID (B820 Inovonics Wireless)

Default: 0
Range: 0 - 99999999
This parameter provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting.
The RFID (**R**adio **F**requency device **Identification** number) is a unique number assigned to a wireless device at the factory. 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 located on the label that is affixed to the device. The label location might differ for each RF device.
RPS Menu Location
SDI2 Modules > Wireless Repeater > RFID (B820 Inovonics Wireless)

RFID (B810 RADION Wireless)

Default: 0
Range: 0 - 99999999
This parameter provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting.
The RFID (**R**adio **F**requency device **Identification** number) is a unique number assigned to a wireless device at the factory. 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 located on the label that is affixed to the device. The label location might differ for each RF device.
RPS Menu Location
SDI2 Modules > Wireless Repeater >RFID (B810 RADION Wireless)

16 Hardware Switch Settings

SDI Keypad Assignments

		DIP Switches					
KP#	Address #	1	2	3	4	5	6
KP 1	Address 1	ON	ON	ON	ON	--	ON
KP 2	Address 2	OFF	ON	ON	ON	--	ON
KP 3	Address 3	ON	OFF	ON	ON	--	ON
KP 4	Address 4	OFF	OFF	ON	ON	--	ON
KP 5	Address 5	ON	ON	OFF	ON	--	ON
KP 6	Address 6	OFF	ON	OFF	ON	--	ON
KP 7	Address 7	ON	OFF	OFF	ON	--	ON
KP 8	Address 8	OFF	OFF	OFF	ON	--	ON
KP 9	Address 9	ON	ON	ON	OFF	--	ON
KP 10	Address 10	OFF	ON	ON	OFF	--	ON
KP 11	Address 11	ON	OFF	ON	OFF	--	ON
KP 12	Address 12	OFF	OFF	ON	OFF	--	ON
KP 13	Address 13	ON	ON	OFF	OFF	--	ON
KP 14	Address 14	OFF	ON	OFF	OFF	--	ON
KP 15	Address 15	ON	OFF	OFF	OFF	--	ON
KP 16	Address 16	OFF	OFF	OFF	OFF	--	ON

DIP Switch 5:

- ON: Encoding Tone On (default)
- OFF: Encoding Tone Off

SDI2 Keypad Assignments (B91x)

		DIP Switches					
KP#	Address #	1	2	3	4	5	6
KP 1	Address 1	ON	OFF	OFF	OFF	OFF	OFF
KP 2	Address 2	OFF	ON	OFF	OFF	OFF	OFF
KP 3	Address 3	ON	ON	OFF	OFF	OFF	OFF
KP 4	Address 4	OFF	OFF	ON	OFF	OFF	OFF
KP 5	Address 5	ON	OFF	ON	OFF	OFF	OFF
KP 6	Address 6	OFF	ON	ON	OFF	OFF	OFF
KP 7	Address 7	ON	ON	ON	OFF	OFF	OFF
KP 8	Address 8	OFF	OFF	OFF	ON	OFF	OFF
KP 9	Address 9	ON	OFF	OFF	ON	OFF	OFF
KP 10	Address 10	OFF	ON	OFF	ON	OFF	OFF
KP 11	Address 11	ON	ON	OFF	ON	OFF	OFF
KP 12	Address 12	OFF	OFF	ON	ON	OFF	OFF
KP 13	Address 13	ON	OFF	ON	ON	OFF	OFF
KP 14	Address 14	OFF	ON	ON	ON	OFF	OFF
KP 15	Address 15	ON	ON	ON	ON	OFF	OFF
KP 16	Address 16	OFF	OFF	OFF	OFF	ON	OFF

D8128 OctoPOPIT Switch Settings

ZONEX 1	D8128D Address Switches					ZONEX 2
Points 9 to 120	1	2	3	4	5	Points 129 to 247
9 to 16	ON	ON	ON	ON	--	129 to 136
17 to 24	ON	ON	ON	OFF	--	137 to 144
25 to 32	ON	ON	OFF	ON	--	145 to 152
33 to 40	ON	ON	OFF	OFF	--	153 to 160
41 to 48	ON	OFF	ON	ON	--	161 to 168
49 to 56	ON	OFF	ON	OFF	--	169 to 176
57 to 64	ON	OFF	OFF	ON	--	177 to 184
65 to 72	ON	OFF	OFF	OFF	--	185 to 192
73 to 80	OFF	ON	ON	ON	--	193 to 200
81 to 88	OFF	ON	ON	OFF	--	201 to 208
89 to 96	OFF	ON	OFF	ON	--	209 to 216
97 to 104	OFF	ON	OFF	OFF	--	217 to 224
105 to 112	OFF	OFF	ON	ON	--	225 to 232
113 to 120	OFF	OFF	ON	OFF	--	233 to 240
121 to 127	OFF	OFF	OFF	ON	--	241 to 247

-- = Line termination switch

NOTE:

- D9112, D9124 and D9412 use points 9-127 on ZONEX 1 and points 129-247 on ZONEX 2.
- A D8128C OctoPOPIT module cannot be configured for points 121-127 and points 241-247. Use a D8125 POPEX module and D9127 POPIT modules for these points.
- The D8128C switch settings are exactly the same as the D8128D. However, the D8128C DIP switches are labeled as 0 through 4 and the D8128D DIP switches are labeled as 1 through 5.
- Set Switch 5 to **On** for line termination.

D9127 POPITs

IMPORTANT:

– The D9412GV4 supports Points 009 to 127
– The D7412GV4 supports Points 009 to 075

ZONEX 1, Points 009 to 048

	DIP Switch						
Address	0	1	2	3	4	5	6
009	ON	ON	ON	ON	ON	ON	ON
010	ON	ON	ON	ON	ON	ON	OFF
011	ON	ON	ON	ON	ON	OFF	ON
012	ON	ON	ON	ON	ON	OFF	OFF
013	ON	ON	ON	ON	OFF	ON	ON
014	ON	ON	ON	ON	OFF	ON	OFF
015	ON	ON	ON	ON	OFF	OFF	ON
016	ON	ON	ON	ON	OFF	OFF	OFF
017	ON	ON	ON	OFF	ON	ON	ON
018	ON	ON	ON	OFF	ON	ON	OFF
019	ON	ON	ON	OFF	ON	OFF	ON
020	ON	ON	ON	OFF	ON	OFF	OFF
021	ON	ON	ON	OFF	OFF	ON	ON
022	ON	ON	ON	OFF	OFF	ON	OFF
023	ON	ON	ON	OFF	OFF	OFF	ON
024	ON	ON	ON	OFF	OFF	OFF	OFF
025	ON	ON	OFF	ON	ON	ON	ON

	DIP Switch						
026	ON	ON	OFF	ON	ON	ON	OFF
027	ON	ON	OFF	ON	ON	OFF	ON
028	ON	ON	OFF	ON	ON	OFF	OFF
029	ON	ON	OFF	ON	OFF	ON	ON
030	ON	ON	OFF	ON	OFF	ON	OFF
031	ON	ON	OFF	ON	OFF	OFF	ON
032	ON	ON	OFF	ON	OFF	OFF	OFF
033	ON	ON	OFF	OFF	ON	ON	ON
034	ON	ON	OFF	OFF	ON	ON	OFF
035	ON	ON	OFF	OFF	ON	OFF	ON
036	ON	ON	OFF	OFF	ON	OFF	OFF
037	ON	ON	OFF	OFF	OFF	ON	ON
038	ON	ON	OFF	OFF	OFF	ON	OFF
039	ON	ON	OFF	OFF	OFF	OFF	ON
040	ON	ON	OFF	OFF	OFF	OFF	OFF
041	ON	OFF	ON	ON	ON	ON	ON
042	ON	OFF	ON	ON	ON	ON	OFF
043	ON	OFF	ON	ON	ON	OFF	ON
044	ON	OFF	ON	ON	ON	OFF	OFF
045	ON	OFF	ON	ON	OFF	ON	ON
046	ON	OFF	ON	ON	OFF	ON	OFF

	DIP Switch						
047	ON	OFF	ON	ON	OFF	OFF	ON
048	ON	OFF	ON	ON	OFF	OFF	OFF

ZONEX 1, Points 049 to 088

	DIP Switch						
Address	0	1	2	3	4	5	6
049	ON	OFF	ON	OFF	ON	ON	ON
050	ON	OFF	ON	OFF	ON	ON	OFF
051	ON	OFF	ON	OFF	ON	OFF	ON
052	ON	OFF	ON	OFF	ON	OFF	OFF
053	ON	OFF	ON	OFF	OFF	ON	ON
054	ON	OFF	ON	OFF	OFF	ON	OFF
055	ON	OFF	ON	OFF	OFF	OFF	ON
056	ON	OFF	ON	OFF	OFF	OFF	OFF
057	ON	OFF	OFF	ON	ON	ON	ON
058	ON	OFF	OFF	ON	ON	ON	OFF
059	ON	OFF	OFF	ON	ON	OFF	ON
060	ON	OFF	OFF	ON	ON	OFF	OFF
061	ON	OFF	OFF	ON	OFF	ON	ON
062	ON	OFF	OFF	ON	OFF	ON	OFF
063	ON	OFF	OFF	ON	OFF	OFF	ON
064	ON	OFF	OFF	ON	OFF	OFF	OFF

	DIP Switch						
065	ON	OFF	OFF	OFF	ON	ON	ON
066	ON	OFF	OFF	OFF	ON	ON	OFF
067	ON	OFF	OFF	OFF	ON	OFF	ON
068	ON	OFF	OFF	OFF	ON	OFF	OFF
069	ON	OFF	OFF	OFF	OFF	ON	ON
070	ON	OFF	OFF	OFF	OFF	ON	OFF
071	ON	OFF	OFF	OFF	OFF	OFF	ON
072	ON	OFF	OFF	OFF	OFF	OFF	OFF
073	OFF	ON	ON	ON	ON	ON	ON
074	OFF	ON	ON	ON	ON	ON	OFF
075	OFF	ON	ON	ON	ON	OFF	ON
076	OFF	ON	ON	ON	ON	OFF	OFF
077	OFF	ON	ON	ON	OFF	ON	ON
078	OFF	ON	ON	ON	OFF	ON	OFF
079	OFF	ON	ON	ON	OFF	OFF	ON
080	OFF	ON	ON	ON	OFF	OFF	OFF
081	OFF	ON	ON	OFF	ON	ON	ON
082	OFF	ON	ON	OFF	ON	ON	OFF
083	OFF	ON	ON	OFF	ON	OFF	ON
084	OFF	ON	ON	OFF	ON	OFF	OFF
085	OFF	ON	ON	OFF	OFF	ON	ON

	DIP Switch						
086	OFF	ON	ON	OFF	OFF	ON	OFF
087	OFF	ON	ON	OFF	OFF	OFF	ON
088	OFF	ON	ON	OFF	OFF	OFF	OFF

ZONEX 1, Points 089 to 128

	DIP Switch						
Address	0	1	2	3	4	5	6
089	OFF	ON	OFF	ON	ON	ON	ON
090	OFF	ON	OFF	ON	ON	ON	OFF
091	OFF	ON	OFF	ON	ON	OFF	ON
092	OFF	ON	OFF	ON	ON	OFF	OFF
093	OFF	ON	OFF	ON	OFF	ON	ON
094	OFF	ON	OFF	ON	OFF	ON	OFF
095	OFF	ON	OFF	ON	OFF	OFF	ON
096	OFF	ON	OFF	ON	OFF	OFF	OFF
097	OFF	ON	OFF	OFF	ON	ON	ON
098	OFF	ON	OFF	OFF	ON	ON	OFF
099	OFF	ON	OFF	OFF	ON	OFF	ON
100	OFF	ON	OFF	OFF	ON	OFF	OFF
101	OFF	ON	OFF	OFF	OFF	ON	ON
102	OFF	ON	OFF	OFF	OFF	ON	OFF
103	OFF	ON	OFF	OFF	OFF	OFF	ON

	DIP Switch						
104	OFF	ON	OFF	OFF	OFF	OFF	OFF
105	OFF	OFF	ON	ON	ON	ON	ON
106	OFF	OFF	ON	ON	ON	ON	OFF
107	OFF	OFF	ON	ON	ON	OFF	ON
108	OFF	OFF	ON	ON	ON	OFF	OFF
109	OFF	OFF	ON	ON	OFF	ON	ON
110	OFF	OFF	ON	ON	OFF	ON	OFF
111	OFF	OFF	ON	ON	OFF	OFF	ON
112	OFF	OFF	ON	ON	OFF	OFF	OFF
113	OFF	OFF	ON	OFF	ON	ON	ON
114	OFF	OFF	ON	OFF	ON	ON	OFF
115	OFF	OFF	ON	OFF	ON	OFF	ON
116	OFF	OFF	ON	OFF	ON	OFF	OFF
117	OFF	OFF	ON	OFF	OFF	ON	ON
118	OFF	OFF	ON	OFF	OFF	ON	OFF
119	OFF	OFF	ON	OFF	OFF	OFF	ON
120	OFF	OFF	ON	OFF	OFF	OFF	OFF
121	OFF	OFF	OFF	ON	ON	ON	ON
122	OFF	OFF	OFF	ON	ON	ON	OFF
123	OFF	OFF	OFF	ON	ON	OFF	ON
124	OFF	OFF	OFF	ON	ON	OFF	OFF

	DIP Switch						
125	OFF	OFF	OFF	ON	OFF	ON	ON
126	OFF	OFF	OFF	ON	OFF	ON	OFF
127	OFF	OFF	OFF	ON	OFF	OFF	ON
128	OFF	OFF	OFF	OFF	OFF	OFF	OFF

ZONEX 2, Points 129 to 168

	DIP Switch						
Address	0	1	2	3	4	5	6
129	ON	ON	ON	ON	ON	ON	ON
130	ON	ON	ON	ON	ON	ON	OFF
131	ON	ON	ON	ON	ON	OFF	ON
132	ON	ON	ON	ON	ON	OFF	OFF
133	ON	ON	ON	ON	OFF	ON	ON
134	ON	ON	ON	ON	OFF	ON	OFF
135	ON	ON	ON	ON	OFF	OFF	ON
136	ON	ON	ON	ON	OFF	OFF	OFF
137	ON	ON	ON	OFF	ON	ON	ON
138	ON	ON	ON	OFF	ON	ON	OFF
139	ON	ON	ON	OFF	ON	OFF	ON
140	ON	ON	ON	OFF	ON	OFF	OFF
141	ON	ON	ON	OFF	OFF	ON	ON

	DIP Switch						
142	ON	ON	ON	OFF	OFF	ON	OFF
143	ON	ON	ON	OFF	OFF	OFF	ON
144	ON	ON	ON	OFF	OFF	OFF	OFF
145	ON	ON	OFF	ON	ON	ON	ON
146	ON	ON	OFF	ON	ON	ON	OFF
147	ON	ON	OFF	ON	ON	OFF	ON
148	ON	ON	OFF	ON	ON	OFF	OFF
149	ON	ON	OFF	ON	OFF	ON	ON
150	ON	ON	OFF	ON	OFF	ON	OFF
151	ON	ON	OFF	ON	OFF	OFF	ON
152	ON	ON	OFF	ON	OFF	OFF	OFF
153	ON	ON	OFF	OFF	ON	ON	ON
154	ON	ON	OFF	OFF	ON	ON	OFF
155	ON	ON	OFF	OFF	ON	OFF	ON
156	ON	ON	OFF	OFF	ON	OFF	OFF
157	ON	ON	OFF	OFF	OFF	ON	ON
158	ON	ON	OFF	OFF	OFF	ON	OFF
159	ON	ON	OFF	OFF	OFF	OFF	ON
160	ON	ON	OFF	OFF	OFF	OFF	OFF
161	ON	OFF	ON	ON	ON	ON	ON
162	ON	OFF	ON	ON	ON	ON	OFF

	DIP Switch						
163	ON	OFF	ON	ON	ON	OFF	ON
164	ON	OFF	ON	ON	ON	OFF	OFF
165	ON	OFF	ON	ON	OFF	ON	ON
166	ON	OFF	ON	ON	OFF	ON	OFF
167	ON	OFF	ON	ON	OFF	OFF	ON
168	ON	OFF	ON	ON	OFF	OFF	OFF

ZONEX 2, Points 169 to 208

	DIP Switch						
Address	0	1	2	3	4	5	6
169	ON	OFF	ON	OFF	ON	ON	ON
170	ON	OFF	ON	OFF	ON	ON	OFF
171	ON	OFF	ON	OFF	ON	OFF	ON
172	ON	OFF	ON	OFF	ON	OFF	OFF
173	ON	OFF	ON	OFF	OFF	ON	ON
174	ON	OFF	ON	OFF	OFF	ON	OFF
175	ON	OFF	ON	OFF	OFF	OFF	ON
176	ON	OFF	ON	OFF	OFF	OFF	OFF
177	ON	OFF	OFF	ON	ON	ON	ON
178	ON	OFF	OFF	ON	ON	ON	OFF
179	ON	OFF	OFF	ON	ON	OFF	ON
180	ON	OFF	OFF	ON	ON	OFF	OFF

	DIP Switch						
181	ON	OFF	OFF	ON	OFF	ON	ON
182	ON	OFF	OFF	ON	OFF	ON	OFF
183	ON	OFF	OFF	ON	OFF	OFF	ON
184	ON	OFF	OFF	ON	OFF	OFF	OFF
185	ON	OFF	OFF	OFF	ON	ON	ON
186	ON	OFF	OFF	OFF	ON	ON	OFF
187	ON	OFF	OFF	OFF	ON	OFF	ON
188	ON	OFF	OFF	OFF	ON	OFF	OFF
189	ON	OFF	OFF	OFF	OFF	ON	ON
190	ON	OFF	OFF	OFF	OFF	ON	OFF
191	ON	OFF	OFF	OFF	OFF	OFF	ON
192	ON	OFF	OFF	OFF	OFF	OFF	OFF
193	OFF	ON	ON	ON	ON	ON	OFF
194	OFF	ON	ON	ON	ON	ON	OFF
195	OFF	ON	ON	ON	ON	OFF	ON
196	OFF	ON	ON	ON	ON	OFF	OFF
197	OFF	ON	ON	ON	OFF	ON	ON
198	OFF	ON	ON	ON	OFF	ON	OFF
199	OFF	ON	ON	ON	OFF	OFF	ON
200	OFF	ON	ON	ON	OFF	OFF	OFF
201	OFF	ON	ON	OFF	ON	ON	ON

	DIP Switch						
202	OFF	ON	ON	OFF	ON	ON	OFF
203	OFF	ON	ON	OFF	ON	OFF	ON
204	OFF	ON	ON	OFF	ON	OFF	OFF
205	OFF	ON	ON	OFF	OFF	ON	ON
206	OFF	ON	ON	OFF	OFF	ON	OFF
207	OFF	ON	ON	OFF	OFF	OFF	ON
208	OFF	ON	ON	OFF	OFF	OFF	OFF

ZONEX 2, Points 209 to 248

	DIP Switch						
Address	0	1	2	3	4	5	6
209	OFF	ON	OFF	ON	ON	ON	ON
210	OFF	ON	OFF	ON	ON	ON	OFF
211	OFF	ON	OFF	ON	ON	OFF	ON
212	OFF	ON	OFF	ON	ON	OFF	OFF
213	OFF	ON	OFF	ON	OFF	ON	ON
214	OFF	ON	OFF	ON	OFF	ON	OFF
215	OFF	ON	OFF	ON	OFF	OFF	ON
216	OFF	ON	OFF	ON	OFF	OFF	OFF
217	OFF	ON	OFF	OFF	ON	ON	ON
218	OFF	ON	OFF	OFF	ON	ON	OFF
219	OFF	ON	OFF	OFF	ON	OFF	ON

	DIP Switch						
220	OFF	ON	OFF	OFF	ON	OFF	OFF
221	OFF	ON	OFF	OFF	OFF	ON	ON
222	OFF	ON	OFF	OFF	OFF	ON	OFF
223	OFF	ON	OFF	OFF	OFF	OFF	ON
224	OFF	ON	OFF	OFF	OFF	OFF	OFF
225	OFF	OFF	ON	ON	ON	ON	ON
226	OFF	OFF	ON	ON	ON	ON	OFF
227	OFF	OFF	ON	ON	ON	OFF	ON
228	OFF	OFF	ON	ON	ON	OFF	OFF
229	OFF	OFF	ON	ON	OFF	ON	ON
230	OFF	OFF	ON	ON	OFF	ON	OFF
231	OFF	OFF	ON	ON	OFF	OFF	ON
232	OFF	OFF	ON	ON	OFF	OFF	OFF
233	OFF	OFF	ON	OFF	ON	ON	ON
234	OFF	OFF	ON	OFF	ON	ON	OFF
235	OFF	OFF	ON	OFF	ON	OFF	ON
236	OFF	OFF	ON	OFF	ON	OFF	OFF
237	OFF	OFF	ON	OFF	OFF	ON	ON
238	OFF	OFF	ON	OFF	OFF	ON	OFF
239	OFF	OFF	ON	OFF	OFF	OFF	ON
240	OFF	OFF	ON	OFF	OFF	OFF	OFF

	DIP Switch						
241	OFF	OFF	OFF	ON	ON	ON	ON
242	OFF	OFF	OFF	ON	ON	ON	OFF
243	OFF	OFF	OFF	ON	ON	OFF	ON
244	OFF	OFF	OFF	ON	ON	OFF	OFF
245	OFF	OFF	OFF	ON	OFF	ON	ON
246	OFF	OFF	OFF	ON	OFF	ON	OFF
247	OFF	OFF	OFF	ON	OFF	OFF	ON
248	OFF	OFF	OFF	OFF	OFF	OFF	OFF

D8129 Octo-relay

ZONEX Bus 1 (Terminals 27 and 28) Output Numbers	S1	S2	S3	S4	S5	ZONEX Bus 2 (Terminals 25 and 26) Output Numbers
1 to 8	Off	On	On	On	On	65 to 72
9 to 16	On	Off	On	On	On	73 to 80
17 to 24	Off	Off	On	On	On	81 to 88
25 to 32	On	On	Off	On	On	89 to 96
33 to 40	Off	On	Off	On	On	97 to 104
41 to 48	On	Off	Off	On	On	105 to 112
49 to 56	Off	Off	Off	On	On	113 to 120
57 to 64	On	On	On	Off	On	121 to 128

D9210C Access Interface

Door Controller	Combined Rotary Switch Settings	Fail Safe Response
Disabled	0	Unlock
1*	81	Unlock
2*	82	Unlock
3	83	Unlock
4	84	Unlock
5	85	Unlock
6	86	Unlock
7	87	Unlock
8	88	Unlock
Door Controller	**Combined Rotary Switch Settings**	**Fail Safe Response**
1*	91	Lock
2*	92	Lock
3	93	Lock
4	94	Lock
5	95	Lock
6	96	Lock
7	97	Lock
8	98	Lock

*The D7412GV4 supports Doors 1 and 2

DX4010i/DX4010V2/DX4020/ITS-DX4020-G

DX4010i/DX4010V2

	DX4010i/DX4010V2 DIP Switches							
Address	1	2	3	4	5	6	7	8
80	Up/ On	Up/ On	Up/ On	Up/ On	Down/ Off	Down/ Off	Down/ Off	Down/ Off
88	Up/ On	Up/ On	Up/ On	Down/ Off	Down/ Off	Down/ Off	Down/ Off	Down/ Off
92	Up/ On	Up/ On	Down/ Off	Down/ Off	Down/ Off	Down/ Off	Down/ Off	Down/ Off

DX4020

	DX4020 DIP Switches							
Address	1	2	3	4	5	6	7	8
80	Down	Down	Down	Down	Up	Up	Up	Up
88	Down	Down	Down	Up	Up	Up	Up	Up
92	Down	Down	Up	Up	Up	Up	Up	Up

ITS-DX4020-G

The Conettix ITS-DX4020-G GPRS/GSM Communicator is not addressed using hardware DIP switches. Instead, the ITS-DX4020-G is configured by:

- sending an SMS message to the ITS-DX4020-G, or
- using the USB connection between a PC and the ITS-DX4020-G

Refer to the *ITS-DX4020-G Installation and Operation Guide* (P/N: F01U133268) for addressing details.

B208 Octo-input Switch Settings

This table describes the relationship between the module switch settings and the point address range that corresponds to the setting. The values of point range listed in this table references back to POINTS > Point Assignments.

IMPORTANT:

- The D9412GV4 supports Points 001 to 247 and modules 1-24.
- The D7412GV4 supports Points 001 to 075 and modules 1-7.
- Terminate unused B208 inputs with an EOL resistor.

B208 Switch Setting	D7412GV4 Point Range	D9412GV4 Point Range
1	11 - 18	11 - 18
2	21 - 28	21 - 28
3	31 - 38	31 - 38
4	41 - 48	41 - 48
5	51 - 58	51 - 58
6	61 - 68	61 - 68
7	71 - 75 *	71 - 78
8		81 - 88
9		91 - 98
10		101 - 108
11		111 - 118
12		121 - 127
13		131 - 138
14		141 - 148
15		151 - 158
16		161 - 168
17		171 - 178
18		181 - 188
19		191 - 198
20		201 - 208
21		211 - 218
22		221 - 228
23		231 - 238
24		241 - 247 *

*For the D9412GV4, only 6 inputs are available at address 24. For the D7412GV4, only 5 inputs are available at address 7.
NOTE: Points 128 and 248 are reserved for supervision of Zonex Buses 1 and 2, and can not be used for modules attached to SDI2.

B308 Octo-output Switch Settings

This table describes the relationship between the module switch settings and the output number range that corresponds to the setting.

IMPORTANT:

- The D9412GV4 supports off-board outputs 001 to 128 and modules 1 - 12.
- The D7412GV4 supports off-board outputs 001 to 64 and modules 1 - 6.
- Not all B308 outputs can be addressed to a control panel output.

B308 Switch Setting	D7412GV4 Output Range	D9412GV4 Output Range
1	11 - 18	11 - 18
2	21 - 28	21 - 28
3	31 - 38	31 - 38
4	41 - 48	41 - 48
5	51 - 58	51 - 58
6	61 - 64 *	61 - 68
7		71 - 78
8		81 - 88
9		91 - 98
10		101 - 108
11		111 - 118
12		121 - 128 *

*For the D7412GV4, only 4 outputs are available at address 6.

B426 (B420) Ethernet Communication Module Switch Settings

This table describes the relationship between the module switch settings and type of control panel communication that corresponds to the setting.

B426 (B420) Switch Setting	Address	Bus Type	Function
0			Local Configuration setting (default setting)
1	1 (173)	SDI2	Automation or RPS, Reporting
2	2 (174)	SDI2	RPS, Reporting
3	80	SDI	Automation
4	88	SDI	RPS, Reporting
5	92	SDI	RPS, Reporting
6	Not applicable for GV4		
7			
8			
9			

B520 Power Supply Switch Settings

The rotary address switch range for the B520 is between 1 and 8. Address ranges 00 and 09-99 are not permissible on the SDI2 device bus. The factory default setting is 01. When using more than one power supply, each power supply must be assigned a different switch setting.

Valid B520 Switch Settings
01
02
03
04
05
06
07
08

B820 Inovonics Wireless Receiver Switch Settings

The B820 address switches provide a single-digit setting for the module's address. The module uses addresses 1 through 4. Addresses 0 and 5 through 9 are invalid.

IMPORTANT: Only address 1 is valid for GV4 Series Control Panels.

B810 RADION Wireless Receiver Switch Settings

The B810 address switches provide a single-digit setting for the module's address. The module uses addresses 1 through 4. Addresses 0 and 5 through 9 are invalid. Only address 1 is valid for the GV4 series control panels.

17 Recommended supervision configuration

To optimize data used for supervision, we recommend the following system settings:

Installation Type	Commercial Burg (UL1610)	Commercial Fire (NFPA 72 2010)	Hourly (NFPA 72 2013)	Medium Security or Household Fire (UL 985)	Daily Supervision
Required Supervision Interval	200 sec	300 sec	1 hr	4 hr	24 hr
Recommended Service Plan	Extended	High Supervision	Standard	Standard	Backup
Panel Programming					
Panel Poll Rate (sec)	140 (2.3 min)	240 (4 min)	3240 (54 min)	12600 (3.5 hr)	64800 (24 hr)
Panel ACK Wait (sec)	10	10	60 (1 min)	300 (5 min)	3600 (1 hr)
Panel Retry Count	5	5	5	5	5
DX4020-G Programming					
GPRS ACK timeout (sec)	70	70	600	600	600
GPRS session timeout (hrs)	4	4	4	4	25 -OR- < carrier timeout

18 Index