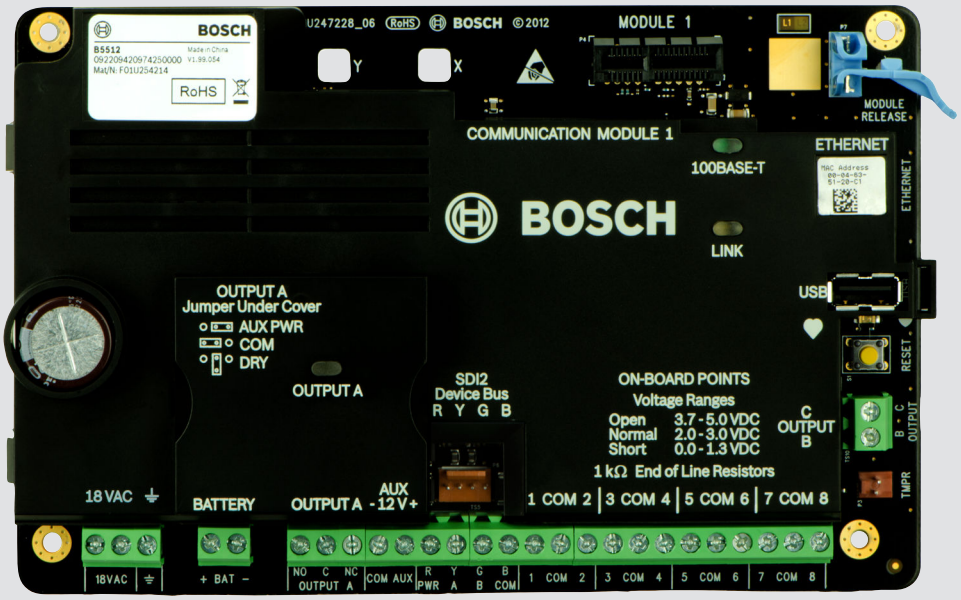


Control Panels

B5512/B4512/B3512

BOSCH

en Program Entry Guide

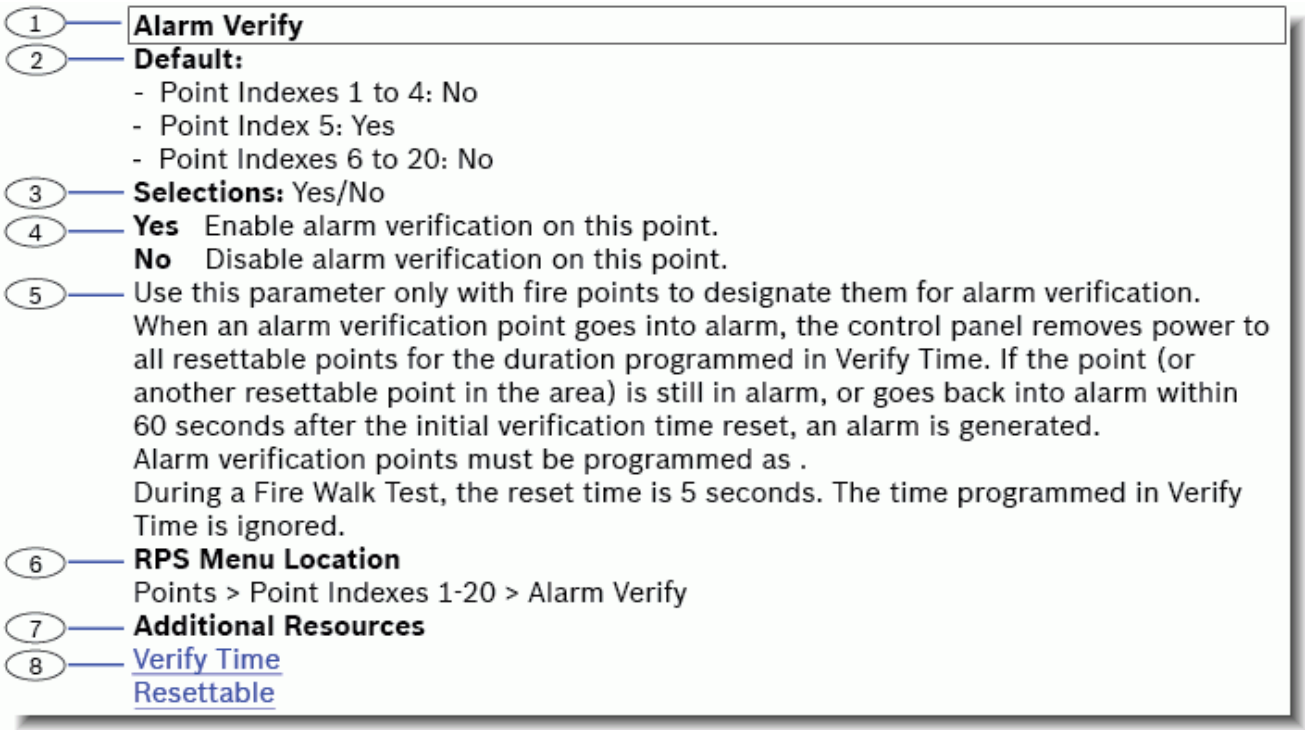
Table of Contents

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.

Callout	Description
4	Selection descriptions. Read the selection descriptions carefully to determine the desired action for this parameter and avoid improperly 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.

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)

Requirement	Parameter
Remote programming shall be disabled (ULC only)	Panel Wide Parameters > RPS Parameters > Answer 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 120 sec	Area Wide Parameters > Exit Delay Time set to less than or equal to 120 sec

Requirement	Parameter
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

Applicable to both IP and cellular communication

Requirement	Parameter
Supervision interval for IP and Cellular 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 and Cellular 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 **Unassigned** and the point with the same number (Point 11 and Output 11 for example) has it's Point Source set to Output.
When Output Source is set to Unassigned, 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 Unassigned 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.

Valid Number Range

	B3512	B4512	B5512
Available virtual output numbers	NA	9-28	9-48
Available virtual point numbers	NA	9-28	9-48

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

3 Panel Wide Parameters

3.1 Phone and Phone Parameters

Phone 1 to 4

Default: Blank
Selections:

Blank The control panel dials no phone number. Leaving this parameter blank does not disable phone routing. To disable reporting to this phone, refer to Routing.

0 - 9 The control panel recognizes these characters as the phone number.

C In some situations, a pause is needed during or immediately after dialing. For example, if the control panel hangs up before it hears the Modem4 ACK tone from the receiver. To insert a pause, program one or more C's in the number sequence where a pause is desired. Each C provides a 3-second pause at the point of insertion.

D The control panel is pre-programmed with a 7-second dial tone detect period. The control panel begins dialing when a dial tone is detected or the waiting period ends. To extend the dial tone detect period, place a D before the phone number.

 # or * These symbols are used for the same purpose as pressing this key on a telephone keypad when manually dialing. For example, an asterisk (*) might be needed to access your long distance service.

This parameter sets the telephone number that the control panel dials to contact the central station receiver when sending reports.
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 to 4

Phone # Format

Default: Modem4
Selections:

Contact ID Use this format when the central station receiver only supports contact ID.

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. Contact ID and 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.

RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > Phone # Format

DTMF Dialing

Default: Yes
Selections:

Yes	Dials the programmed phone numbers using touch-tone/DTMF (dual-tone multi-frequency).
No	Use for pulse dialing only.

This parameter dials the central station receiver phone number for event reports and/or RPS.
RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > DTMF Dialing

Phone Supervision Time

Default: 0
Selections:

0	No phone line supervision.
10-240 (sec)	Enter the number of seconds (in 10 second increments) to supervise the phone line.

This parameter sets the length of time the control panel continues to monitor a faulted phone line before initiating phone line trouble responses.
The control panel tests the phone line approximately nine times a minute.
Keypads display the number of the phone line that has failed. The keypad initiates a trouble tone if both Buzz On Fail and Trouble Tone are set to Yes.
After a faulted phone line restores, it takes the same amount of time to initiate restoral responses. 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.
RPS Menu Location
Panel Wide Parameters > Phone and Phone Parameters > Phone Supervision Time

Additional resources
Buzz On Fail

Alarm On Fail

Default: No
Selections:

Yes	This option generates alarm responses when the phone line fails.
No	Phone failures report as trouble responses for Area 1 and/or the account number for Area 1.

This parameter activates the Area 1 Burglar Bell if the phone line fails.
Phone Supervision 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.
RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > Alarm on Fail

Buzz On Fail

Default: No
Selections:

Yes Generates panel-wide trouble tones and displays the event at keypads when a Phone Fail event occurs.

No The Phone Fail event displays at the keypads, but no trouble tone is generated.

This parameter activates the Trouble Tone if the phone line fails.
Phone Supervision Time must be programmed to use this feature. Panel-wide trouble tones for individual keypads (based on their KP# 1 through 8) can be turned off by programming Trouble Tone in Keypad Parameters as NO.
RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > Buzz On Fail
Additional resources
Phone Supervision Time

Expand Test Report

Default: No
Selections:

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 events for the events listed in the routing group test reports at test time.

This parameter is used to add system event information to test reports. Test reports can be set up as manual test reports or as scheduled events in the Skeds section of the program.
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.
RPS Menu Location:
Panel Wide Parameters > Phone and Phone Parameters > Expand Test Report

3.2 Onboard Ethernet Communicator

IPv6 Enable

Default: No
Selections:

Yes Enable IPv6.

No Disable IPv6 (IPv4 mode being used).

This parameter sets which mode is being used.
When IPv6 Enable is set to Yes:
– IPv4 parameters are Read Only.
– The IPv4 address, IPv4 subnet mask, and IPv4 Default Gateway are locked (i.e. grayed out and not editable).
– The DHCP/AutoIP enable should be set to Yes.
When IPv6 Enable is set to No, IPv6 parameters are Read Only.
RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Enable
SDI2 > IP Communicator > IPv6 Enable

IPv4 DHCP/AutoIP Enable

Default: Yes
Selections:

Yes Enable DHCP to automatically configure the IP Address, IP Default Gateway, and IP DNS Server Address.

No Manually configure the Onboard Ethernet Communicator. Use this setting if there is no DHCP service.

This parameter configures the Onboard Ethernet communicator automatically using DHCP
DHCP allows a computer to be automatically configured which eliminates the need for interaction by a network administrator. DHCP also provides a central database that tracks computers that connect to the network, which prevents two computers from accidentally being configured with the same IP address.
AutoIP enables dynamic IP addresses to be assigned to a device when the device is started up. DHCP requires a DHCP server.
When Yes is selected, the IPv4 address, IPv4 Subnet Mask, and IPv4 Default Gateway are grayed out and cannot be changed.
When No is selected, IPv6 Mode should be set to No.
Note: If IPv6 Enable is set to Yes, then this option is not available. The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DHCP/AutoIP Enable
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 Ethernet communication method if DHCP is disabled.
If IPv4 DHCP/Auto IP Enable is not selected than this must be configured.
The IPv4 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 of 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:
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 address
SDI2 Modules > IP Communicator > IPv4 address

IPv4 Default Gateway

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter configures the address of the local network gateway to the Internet or Intranet.

A gateway is a point on a TCP/IP network that serves as an entrance to another network. A host uses a default gateway when an IP packet's destination address belongs to someplace outside the local subnet. The default gateway address is usually an interface belonging to the LAN's border router. In DHCP mode, the default gateway is usually resolved automatically. When DHCP/AutoIP Enable is set to Yes, this parameter cannot be changed. Leave the default value.
The parameter has no effect on B450 operation.

RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Default Gateway
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.
A Domain Name Server (DNS) converts internet domain names or hostnames 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 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.

RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DNS server IP address
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:FFFF: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 hostnames to their corresponding IP addresses. In DHCP mode, the default value indicates that 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 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 Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DNS server IP address
SDI2 Modules > IP Communicator > IPv6 DNS server IP address

UPnP (Universal Plug and Play) Enable

Default: Yes
Selections:

Yes Enable IP devices to connect on the network.

No Disable IP devices from connecting on the network.

This parameter allows IP devices to discover each other's presence on the network and connect for communication. This parameter also allows a router to forward port numbers through the keypad itself, allowing reports to reach receivers behind the router.
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > UPnP (Universal Plug and Play) Enable
SDI2 Modules > IP Communicator > UPnP (Universal Plug and Play) Enable

ARP Cache Timeout

Default: 600
Selections: 1 to 600 (seconds)
This parameter specifies the time-out for ARP cache entries (time-out value in seconds).
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > ARP Cache Timeout
SDI2 Modules > IP Communicator > ARP Cache Timeout

Module Hostname

Default: Blank
Selections: Up to sixty-three characters (Letters, Numbers, and Dashes)
This parameter allows the user to customize a module hostname. This is the hostname that represents the communication device on the network.
Optionally, use the hostname to contact the control panel via RPS over network, for Remote Security Control, or for module web configuration and diagnostics.
IMPORTANT
- If this field is left blank, Ethernet communicator module will determine its hostname based on its MAC address (the factory default hostname).
- Use the hostname on a local network using DHCP. To use the hostname externally, enter the hostname in the DNS server.

The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Module Hostname
SDI2 Modules > IP Communicator > Module Hostname

TCP/UDP Port Number

Default: 7700
Selections: 0 - 65535
This parameter sets the local port number that the module listens for in-coming network traffic. This port is also the source for outgoing communications.

The TCP/UDP Port is typically configured as 7700 when the control panel is communicating with a central station receiver, RPS, Automation, or Remote Security Control (RSC). 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.

RPS Menu Location
Panel Wide Parameters > Onboard Ethernet Communicator > TCP/UDP Port Number

TCP Keepalive Time

Default: 45
Selections: 0 - 65 (seconds)
This parameter sets 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.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > TCP Keepalive Time
SDI2 Modules > IP Communicator > TCP Keepalive Time

IPv4 Test Address

Default: 8.8.8.8
Selections: IPv4 address or Domain Name
This parameter sets the IPv4 Test Address. The IPv4 Test Address is used by the Onboard Ethernet communicator connection to ping an internet address in order to verify the integrity of the network and the network configuration setting.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Test Address
SDI2 Modules > IP > IPv4 Test Address
Additional resources:
Network Address Format

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 Onboard Ethernet communicator 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
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Test Address
SDI2 Modules > IP Communicator > IPv6 Test Address
Additional resources:
Network Address Format

Alternate IPv4 DNS server IP address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter provides an alternate IPv4 DNS server IP address.
If the module fails to obtain an address from the primary server, the alternate DNS server is used if one has been specified. The Alternate 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 Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv4 DNS server IP address
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.
The Alternate 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 has a value between 0000-FFFF. When this is defined through the DHCP service, leave the default value. If the module fails to obtain an address from the primary server, the Alternate IPV6 DNS server is used, if specified. The module can use the Alternate IPv6 DNS server only when the Primary address is not the default address.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv6 DNS server IP address
SDI2 > IP Communicator > Alternate IPv6 DNS server IP address

3.3 Cellular Plug-in Module

IMPORTANT CELLULAR SERVICE INFORMATION
Refer to Configuring for Cellular Communication for important information regarding how to set up your control panel to ensure proper cellular communication with the central station receiver.

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
Panel Wide Parameters > Cellular Plug-in Module > Inbound SMS
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inbound SMS

Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Session Keep Alive Period
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Session Keep Alive Period
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Inactivity Timeout
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inactivity Timeout
Additional Information
Configuring for Cellular Communication

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

Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Low Signal Strength
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Low Signal Strength

Additional Information

Configuring for Cellular Communication

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

Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for No Towers
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for No Towers

Additional Information

Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Single Tower
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Single Tower
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Outgoing SMS Length
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Outgoing SMS Length
Additional Information
Configuring for Cellular Communication

Network Access Point Name

Default: data421d.com
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
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Name
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point User Name
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point User Name
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Password
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point Password
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > SIM PIN
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > SIM PIN
Additional Information
Configuring for Cellular Communication

3.4 IP Cameras

Camera Name

Default: Camera #
Selections: 0-32 characters
This parameter allows the user to enter a description for the Bosch IP camera selected. Enter up to 32 characters of text, numbers, and symbols.

IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Camera Name

Camera Name (second language)

Default: Blank
Selections: Enter up to 32 characters.
This parameter allows the user to enter a description for the Bosch IP camera selected. Enter up to 32 characters from the Latin-1 8-bit (ISO/IEC 8859-1) character set to describe the area.
Note: First and Second languages are programmed during panel account setup in the Panel Data window. Supported languages include English, Spanish, French and Portuguese. To view the languages selected during account set-up, refer to Panel Wide Parameters > Personal Notification > User Language.

IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Camera Name (second language)

URL or IP Address

Default: Blank
Selections: 0-128 ASCII characters
This parameter sets the URL or IP address for the indicated Bosch IP camera.
The control panel uses the URL or IP address to communicate with the camera over a network.

IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > URL or IP Address

3.4.1 Bosch Connected Cameras

Bosch IP Camera Overview

Products
– B Series control panels with IP
– All Bosch IP cameras

Applications
Bosch IP cameras are best for small commercial and residential applications where conventional video integration hardware and applications are cost prohibitive.

Implementation
The B Series control panel communicates with Bosch IP cameras using a low-level language (RCP+).
Configure B Series control panels to use Bosch IP cameras as inputs, outputs, or both.

Environment
Install B Series control panels and Bosch IP cameras on the same network (LAN).

Panel Configuration
Configure the control panel with each camera's IP address. RCP+ port #, Service password, and Supervision period (sec) parameters configure network communication and supervision with connected Bosch IP cameras..

Other panel configuration for using IP cameras
New Point Source option "IP Camera" (ref. Points > Point Assignments > Source)
New Output Source option "IP Camera" (ref. Output Parameters > Output Configuration > Output Source)

RCP+ Port

Default: 1756
Selections: 0-65535
This parameter assigns an RCP+ port number for the path used for a Bosch IP camera to communicate with the control panel over a network.

IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Port #

Service Password

Default: Blank
Selections: 0, 1-32 characters
0 = Disable feature
This parameter sets the password required to access the Bosch IP camera's data. The password is case sensitive.

IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Service Password

Supervision Period (sec)

Default: 0
Selections: 0, 10-128 sec
0 = Disable supervision
This parameter sets the length of time the control panel monitors a missing Bosch IP camera before reporting the camera as missing.

IMPORTANT:
– This parameter has no effect if no inputs or outputs are assigned to the IP camera.
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Supervision Period

3.4.2 Live (Video)

Live (Video) Overview

Products
- B Series control panels with IP
- All Bosch IP cameras
- RSC (Remote Security Control)

Applications
Live video is best for small commercial and residential applications where conventional video integration hardware and applications are cost prohibitive.

Implementation
The B Series control panel communicates with Bosch IP cameras using a low-level language (RCP+).
Configure B Series control panels to use Bosch IP cameras as inputs, outputs, or both.
The device configuration is independent, but native.

Environment
Install B Series control panels and Bosch IP cameras on the same network (LAN).

Panel Configuration
RSC uses the Port #, Use HTTPS?, User Name, and Password parameters to access video images within the IP cameras.

Port

Default: 80
Selections: 0-65535
This parameter assigns a port number for the path the RSC application uses to communicate with the camera and view live video feed.
If the live viewer URL is assigned to a router, configure the router with the value specified here.
IMPORTANT:
- Only the B5512 and B4512 control panels support this parameter.
- The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > Port #

Use HTTPS?

Default: No
Selections:

Yes	Enable HTTPS
No	Disable HTTPS

Use this parameter to encrypt data for a secure network communications between the Bosch IP camera and the control panel.
Set to "Yes" if the live viewer requires HTTPS.
RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > Use HTTPS?

User Name

Default: live
This parameter specifies the user name that the RSC application uses to show video from the camera.
RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > User Name

Password

Default: Blank
Selections: 0-32 characters
This parameter sets the password required by the RSC application to view video from the camera. The password is case sensitive.
IMPORTANT:
– Only the B5512 and B4512 control panels support this parameter.
– The B5512 supports Cameras 1-4. The B4512 supports Cameras 1 and 2.
RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > Password

3.5 Report Routing

Report Routing Overview

Routing lets you select full or partial groups of events to be reported to up to four different destinations. Routing includes choosing which is the highest priority destination, which events are reported to a single or multiple destination and if the events fail, which backup destination should be selected.
Route Groups
To program a route group, first choose a Route Group number. The lower the Route Group number, the higher priority that group has (example: events in Route Group 1 have a higher priority than those in Route Group 2, 3 or 4 if each group has a report to send at the same time). This is important when programming duplicate reports or choosing which events you want to ensure are reported first. Remember, Route Group 1 Primary Path Device will be the first destination that the control panel if an event in that group needs to be reported. If the control panel is idle, any event generated for any group initiates communication.
Assigning Reports to Multiple Route Groups
To allow an event within a group to report to multiple groups, the event should be YES for each Route Group. For instance, programming Fire Alarms for Route Group 1 and Route Group 2 results in the fire alarms reporting to Route Group 1 first, followed by a duplicate report to Route Group 2.
Prioritizing Reports within a Route Group
Fire alarm events have the highest priority and are reported first for each group. The next highest priority events are in the following order, gas, panic, duress, medical, intrusion alarm, supervisory and then all troubles and restorals.
Note: When individual events have been manually enabled or disabled for reporting in a route group, the setting displays as Custom.

Fire Reports

Default:
- Route Groups 1-3: Yes
- Route Group 4: Custom

Selections:

Yes Enable reporting on all fire events.

No Disable reporting on all fire events.

This parameter enables or disables reporting on fire events. Use this parameter to manually select which fire function events to enable or disable reporting on.
Fire Reports can be programmed for up to four route groups. Parameters available within each route group are:
- Fire Alarm Reports fire alarm.
- Fire Restoral (After Alarm) Reports fire restoral from alarm.
- Fire Missing Reports missing fire point.
- Fire Trouble Reports fire trouble.
- Fire Supervision Reports fire supervisory.
- 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.

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

Gas Reports

Default:
- Route Groups 1-3: Yes
- Route Group 4: Custom

Selections:

Yes Enable reporting on all gas events.

No Disable reporting on all gas events.

This parameter enables or disables reporting on gas events. Use this parameter to manually select which gas function events to enable or disable reporting on.
Gas Reports can be programmed for up to four route groups. Parameters available within each route group are:
- 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 supervisory.
- 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.

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

Burglar Reports

Default:
– Route Groups 1-3: Yes
– Route Group 4: Custom

Selections:

Yes Enable reporting on all burglar events.

No Disable reporting on all burglar events.

This parameter enables or disables reporting on burglar events. Use this parameter to manually select which burglar function events to enable or disable reporting on.
Parameters within this route group are:
– 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 supervisory 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).
The Unverified Event is sent when a single point programming in Cross Point Group faults into an alarm event, 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.

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

Personal Emergency Reports

Default:
– Route Groups 1-3: Yes
– Route Group 4: Custom

Selections:

Yes Enable reporting on all personal emergency events.

No Disable reporting on all personal emergency events.

This parameter enables or disables reporting on personal emergency events. Use this parameter to manually select which personal emergency function events to enable or disable reporting on.
Parameters within this route group are:
Medical Alarm
Medical Alarm Restoral
Silent / Hold-Up Alarm

Silent / Hold-Up Alarm Restoral
Panel Wide Parameters > Report Routing > Personal Emergency Reports.
Panic Alarm
Panic Alarm Restoral
RPS Menu Location
Panel Wide Parameters > Report Routing > Personal Emergency Reports.

User Reports

Default: Custom
Selections:
Yes Enable reporting on all user events.

No Disable reporting on all user events.

This parameter enables or disables reporting on user events. Use this parameter to manually select which user function events to enable or disable reporting on.
Parameters within this route group are:
– 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 armed event.
– Forced Close Part On Delay: Reports forced close part on, delay armed 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:
– Route Groups 1-3: Yes
– Route Group 4: No
Selections:
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 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 when some diagnostic 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
SDI2 Device Failure[1, 5]	**Yes**, No	SDI2 device failure.
SDI2 Device Restoral	**Yes**, No	Restoral of SDI2 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.

Report	Selections	Report Description
AC Failure[1,]	**Yes**, No	Failure of AC power to control panel.
AC Restoral	**Yes**, No	Restoral of AC power to control panel after failure.
Battery Missing[1,]	**Yes**, No	Battery missing detection event.
Battery Low[1,]	**Yes**, No	Low battery power.
Battery Restoral	**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.
Route 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	**Yes**, No	Reports on occurrence of an RF smoke detector failure

Report	Selections	Report Description
Service Smoke Detector Restoral	Route Comm Fail: **Yes**, No	Reports restoral from an occurrence.
Send Version Text	**Yes**, No	Send Control Panel and Bootloader Firmware versions with Reboot events.

[1] = Indicates an off-normal event.
[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.
[5] = Includes cellular trouble events.

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

Output Reports

Default:
– Route Groups 1-3: Yes
– Route Group 4: Custom

Selections:
Yes Enable reporting on all output events.

No Disable reporting on all output events.

This parameter enables or disables reporting on output events. Use this parameter to manually select which Outputs to enable or disable reporting on.

IMPORTANT: For Sensor Reset, the control panel logs the event as follows regardless if the output is activated locally from a keypad or remotely from RPS: Output 253 [Output A(1)], Output 254 [Output B(2)], and Output 255 [Output C(3)].

Parameters within this route group are:
– Sensor Reset. Reports sensor reset event.
– Output Set. Reports output set event.
– Output Reset. Reports output reset event.
– Send Output Name Text.

When activating an on-board output using remote automation software, the control panel logs the events

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

Auto Function Reports

Default:
– Route Groups 1-3: Yes
– Route Group 4: No

Selections:
Yes Enable reporting on this auto function event.

No Disable reporting on this auto function event.

Custom This setting cannot be selected by the user. It is displayed automatically whenever some diagnostics reports are enabled and others are disabled.

This parameter enables or disables reporting on a variety of automatic functions. Use this parameter to manually select which auto function events to enable or disable reporting on.
Parameters within this route group are:
– Sked Executed. Reports Sked executed event.
– Sked Changed. Reports Sked changed event.
– Fail to Execute. Reports a fail to execute event.

RPS Menu Location
Panel Wide Parameters > Report Routing > Auto Function Reports.

RPS Reports

Default:
– Route Groups 1-3: Yes
– Route Group 4: No

Selections:

Yes Enable reporting on all RPS events.

No Disable reporting on all RPS events.

This parameter enables or disables reporting on RPS events. Use this parameter to manually select which RPS function events to enable or disable reporting on.

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.

Parameters within this route group are:
– 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:
– Route Groups 1-3: Yes
– Route Group 4: No

Selections:

Yes Enable reporting on all point events.

No Disable reporting on all point events.

This parameter enables or disables reporting on point events. Use this parameter to manually select which point function events to enable or disable reporting on.
Parameters within this route group are:
– Service Start. Reports service walk test start event.
– Service End. Reports service walk test end event.
– Fire Walk Start. Reports fire walk start event.
– Fire Walk End. Reports fire walk end event.
– Walk Test Start. Reports walk test start event for walk test and invisible walk test.
– Walk Test End. Reports walk test end event for walk test and invisible walk test.
– Extra Point. Reports extra point event.
– Send Point Text. Reports point text.
– RF Low Battery. Reports RF point low battery events.
– RF Low Battery Restore. Reports restoral from RF point low battery events.
– 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:
– Route Groups 1-3: Yes
– Route Group 4: No

Selections:

Yes Enable reporting on all user change events.

No Disable reporting on all user change events.

This parameter enables or disables reporting on user changes. Use this parameter to manually select which user change function events to enable or disable reporting on.
Parameters within this route group are:
– 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.
– Keyfob Assigned. Reports card assigned or RADION keyfob assigned to user event.
– Keyfob Removed. Reports when a RADION keyfob assignment is removed from a user.

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

3.6 Communicator

Communicator Overview

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 used to send the report. The backup path device is used if the primary path device fails.

The control panel makes up to ten communication attempts using the primary and backup path devices to send a report within a route group. The control panel alternates between the primary and backup path devices as shown in the table below. If unsuccessful, it creates a Comm Fail Event.

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 to that device. When both primary and backup paths are configured for "Phone", it might take up to 10 minutes for the control panel to go in to Comm Fail (create a Comm Fail event).
By setting a primary or backup path device to an Onboard Ethernet communicator path or SDI2 path, the module automatically becomes supervised. Any loss of bus communication results in an SDI2 Fail system fault.

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 control 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 control panel dials the number anyway. Each time the number is dialed, the control panel records this as an attempt. After 10 attempts the control panel goes into Communications Failure and displays the event on the keypads.

Programming a Primary and Backup Destination
Each Route Group has a Primary Path Device and a Backup Path Device . In applications where two phone numbers are programmed, the Primary Path Device destination is the Phone # that the Route Group attempts to dial first. If the Primary Path Device destination fails to connect to the central station receiver after two dialing attempts, the Backup Path Device destination is dialed. In addition to this, the control panel can be programmed such that the Primary Path Device and/or the Backup Path Device are an SDI2 device, such as a Network Interface Module or Ethernet Interface Module. The control panel can also be programmed to attempt only once for the Primary Path Device before attempting to send events using the Backup Path Device.

Routing Destination Communication Failures
When the Primary Path Device fails to connect to the Central Station receiver after two attempts, the Backup Path Device attempts to connect. The central station receives the original event with a COMM TROUBLE PHONE # =(1, 2, 3, or 4) report added. This event does not occur if no Backup Path Device is designated.. COMM RESTORE events are generated.
If the Primary Path Device is an IP Path, the central station receives the original event with a COMM TROUBLE RG8 SDI2## event modifier.

Device	Path 1	Path 2	Path 3	Path 4
SDI2-1	11	21	31	41
Onboard Ethernet	10	20	30	40
Onboard Cellular	18	28	38	48

When all attempts to both the primary path device and backup path device fail, a COMM FAIL RG# event is generated. COMM RESTORE events are not generated. The same COMM TROUBLE events 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.

Communication Attempts
The primary path device within a group will make six individual attempts to communicate and the backup path device will make four attempts to communicate 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.

Detecting Panel Substitution
Ethernet and cellular alarm communications to the central station have anti-substitution keys built-in, such that a replayed message or panel substitution can be detected by the central station receiver.

Network Address Format

The Network Address defines an IPv4, IPv6 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 or IPv6) Format
This is in ASCII decimal format: xxx.xxx.xxx.xxx
Example:
Correct 12.23.145.251
Incorrect 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 resources:
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
- Onboard IP Path 1
- Onboard IP Path 2
- Onboard IP Path 3
- Onboard IP Path 4
- Cellular IP Path 1
- Cellular IP Path 2
- Cellular IP Path 3
- Cellular IP Path 4
- Phone 1
- Phone 2
- Phone 3
- Phone 4
- SDI2 address 1 Path 1
- SDI2 address 1 Path 2
- SDI2 address 1 Path 3
- SDI2 address 1 Path 4

This parameter sets the communication device and destination path combination that the control panel uses as its primary routing path to send reports to the central station receiver.
You cannot select the same path and device combination for both Primary and Backup Path for a route group.
RPS Menu Location:
Panel Wide Parameters > Communicator > Primary Path Device
Additional Resource:
For more information on paths, refer to Communicator – Overview.

Backup Path Device

Default: No Device
Selections:
- No Device
- Onboard IP Path 1
- Onboard IP Path 2
- Onboard IP Path 3
- Onboard IP Path 4
- Cellular IP Path 1
- Cellular IP Path 2
- Cellular IP Path 3
- Cellular IP Path 4
- Phone 1
- Phone 2
- Phone 3
- Phone 4
- SDI2 address 1 Path 1
- SDI2 address 1 Path 2
- SDI2 address 1 Path 3
- SDI2 address 1 Path 4

This parameter sets the communication device and destination path combination that the control panel uses as its primary routing path to send reports to the central station receiver.
You cannot select the same path and device combination for both Primary and Backup Path for a route group. The backup path is used when the primary path fails.
RPS Menu Location:
Panel Wide Parameters > Communicator > Backup Path Device.
Additional resources:
For more information on paths, refer to Communicator – Overview.

RG Same Network Receiver

Default: Yes
Selections:

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

This parameter defines whether the primary and backup IP paths for a Route Group go to the same central station receiver.

The Route Group Same Network Receiver feature 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 event. Set this parameter to Yes when the following events apply:

- Both primary and backup devices use enhanced communication via an IP path (on-board or SDI2).
- 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 event.

If the poll rate is set to 5 minutes or faster, there is a possibility of excessive data usage that might exceed your data plan with the cellular service provider. Be sure that any Communication Trouble events are addressed as soon as possible.

RPS Menu 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.

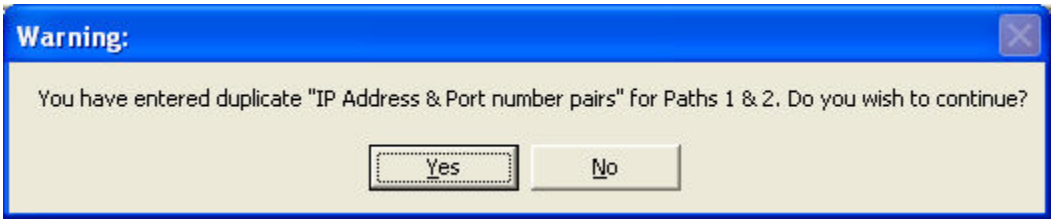
Off by More than 30 Minutes:
The control panel checks for a date change. If the day, month, or year has changed, the control panel's date is set to the new date. The control panel then sets its time to

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

3.7 Enhanced Communication

Network Address

Default: Blank
Selections: IPv4 Address (0.0.0.0 to 255.255.255.255) or Hostname (Up to 255 Characters)
This parameter sets the IP address for Paths 1-4.
There are four available Paths to route events to.
If events are going to be routed to an IP Address (in a Private Local or Wide Area Network application), you need to determine which Path to use (Path 1 – Path 4) and enter the appropriate IP Address for that Path.
Whenever the central station requests a change to the IP Address or Port Number configured in the control panel, the central station receiver might resynchronize the control panel's anti-replay/anti-substitution static key.
When Port Number/IP Address pairs have duplicate values in a 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.



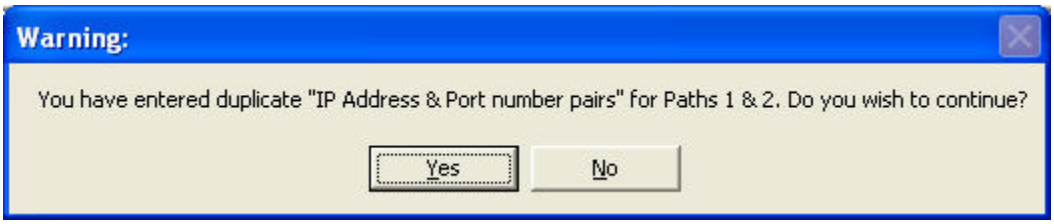
RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > Network Address (Paths 1-4)

Additional resources:
Network Address Format

Port Number

Default: 7700
Selections: 1 to 65,535
This parameter assigns a unique port number for each path used to communicate with the central station over a network.
When upgrading a non-control panel account to a 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 might resynchronize the control panel's anti-replay/anti-substitution static key.
When Port Number/IP Address pairs have duplicate values in a 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.



RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > Port Number (Paths 1-4)

Receiver Supervision Time

Default: 4 Hours
Selections:

200 Sec	Commercial Burg
300 Sec	NFPA 72 2010
1 Hr	NFPA 72 2013
4 Hrs	Medium Security
24 Hrs	Daily
25 Hrs	
90 Sec	High Security
No Polling	
95-195, 205-1275 Sec	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 Hrs	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. Refer to the Recommended supervision configuration table.

WARNING: This parameter is critical for optimized communication. Refer to Configuring for Cellular Communication for important information regarding how to set up your control panel to ensure proper cellular communication with the central station receiver.

Poll Rate

Default: 12600

Selections:

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.

This parameter is used to set the interval (in seconds) in which each SDI2 path sends a heartbeat poll to the central station receiver for supervision purposes. This ensures the integrity of the connection at all times.

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 SDI2 ## event. (Refer to the table below for the correct ## value.)

Device	Path 1	Path 2	Path 3	Path 4
SDI2-1	11	21	31	41

Device	Path 1	Path 2	Path 3	Path 4
Onboard Ethernet	10	20	30	40
Onboard Cellular	12	22	32	42

Poll Rate (Paths 1 to 4), ACK Wait Time (Paths 1 to 4), and Retry Count (Paths 1 to 4) determine how the network path is supervised between the communication device and the central station receiver(s). Do not confuse the SDI2 path supervision with the supervision of the SDI2 device itself (the connection of the SDI2 device to the control panel).
If this parameter is programmed with a value and the central station does not acknowledge the poll from the control panel, keypads sound a trouble event. 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 network 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

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 event occurs, all events routed to this path go immediately to the backup path.
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 SDI2 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 from less than 300 seconds to 300 seconds when online with RPS. The poll rate returns to the programmed value after the RPS session ends.

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > Poll Rate (Paths 1-4)

Additional Information
ACK Wait Time (Paths 1 to 4)
Retry Count (Paths 1 to 4)
Comm Fail

ACK Wait Time

Default: 300
Selections: 5 to 65535 (seconds)
This parameter determines how long the control panel waits for an acknowledgement from the central station after a heartbeat poll or an actual event has been transmitted. Actual (non-heartbeat) events wait the set period of time or a maximum of 15 seconds before the next communication attempt is made.

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > ACK Wait Time

Additional Information
Poll Rate
Retry Count (Paths 1 to 4)

Retry Count

Default: 5
Selections:

0 Path failure events are not generated.

1 to 255 Path failure events are generated after the number of retries are reached for a given SDI2 Path.

This parameter determines how many times the control panel will re-send the heartbeat event before declaring a Path Failure.
An event is defined by the following device and path combinations.

Device	Path 1	Path 2	Path 3	Path 4
SDI2-1	11	21	31	41
Onboard Ethernet	10	20	30	40
Onboard Cellular	18	28	38	48

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > Retry Count

Additional Information
Poll Rate
ACK Wait Time

AES Key Size

Default: No Encryption
Selections: No Encryption, 128, 192, 256 (bits)
This parameter identifies the AES key size.
– 128 bit key length is 16 bytes.
– 192 bit key length is 24 bytes.
– 256 bit key length is 32 bytes.
RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > AES Key Size

AES Encryption Key

Default: <Default> (not encrypted)
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.
RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > AES Encryption Key
Additional resources:
AES key strings are configured in Config >> System >> Encryption Key Tab

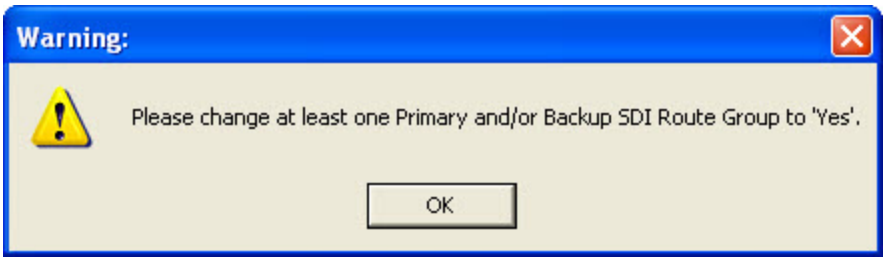
3.8 SDI2 RPS/Enhanced Communication

Enable Enhanced Communication

Default: Yes
Selections:

Yes	Event routing occurs using an IP path as the communications channel.
No	Event routing occurs using a PSTN connection as the communication channel.

This parameter sets the communication channel for event routing.
In order to select Yes as a configuration option, one of the four Primary or Backup SDI2 Route groups should be set to an SDI2 or Onboard Ethernet communicator path. If a Primary or Backup Route group is not set properly the following dialog will be displayed.



RPS Menu Location
Panel Wide Parameters > SDI2 RPS / Enhanced Communications > Enable Enhanced Communication.

Additional resources
To set SDI2 Route Groups, refer to Primary Path Device or Backup Path Device.

Answer RPS Over Network?

Default: Yes
Selections:

Yes This setting enables automatic answering of RPS initiated sessions over the network.

No This setting prevents automatic answering of RPS initiated sessions over the network.

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

This parameter determines if the control panel automatically answers RPS initiated sessions through a network interface module on the SDI2 bus or onboard Ethernet communicator.

This parameter can be momentarily disabled by selecting ALLOW ANSWER through the Remote Programming menu.

RPS Menu Location
Panel Wide Parameters > SDI RPS/Enhanced Communication > Answer RPS Over Network.

RPS Address Verification

Default: No
Selections:

Yes This setting verifies that the incoming RPS IP address matches the address entered in RPS Network Address.

No This setting allows RPS to connect to the control panel from any IP address. No verification is performed.

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.

RPS Menu Location
Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Address Verification.

RPS Network Address

Default: Blank
Selections: IPv4 address or Hostname
This parameter sets 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.
RPS Menu Location
Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Network Address.

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.
RPS Menu Location
Panel Wide Parameters > SDI RPS/Enhanced Communication > RPS Port Number

3.9 Power Supervision

AC Fail Time

Default: 01:00
Selections: 00:01 to 90:00 (Minutes:Seconds)
This parameter sets the amount of time that the AC power must be off before the control panel sends an AC Failure report.
RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Fail Time.

Resend AC Fail

Default: No Reports
Selections: No Reports, After 6 Hours, After 12 Hours
No Report Do not re-send AC Fail report.

After 6 Hours Re-send AC Fail report to central station after 6 hours of non-restoral.

After 12 Hours Re-send AC Fail report to central station after 12 hours of non-restoral.

This parameter sets the time interval that must pass without the AC failure event being restored before the control panel re-sends the AC Failure report to the central station.
RPS Menu Location
Panel Wide Parameters > Power Supervision > Resend AC Fail.

AC Fail Display

Default: 60
Selections: 10 to 300 (seconds) (increments of 5)
This parameter sets 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- control panel account to a control panel account, RPS forces the default to **60 seconds**.

RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Fail Display.

AC Fail/Restoral Report

Default: No
Selections:
Yes Send AC Fail and AC Restoral reports.

No Do not send AC Fail and AC Restoral reports.

This parameter sends AC Power Supervision reports to the central station at the time programmed for ***AC Fail Time***.
RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Fail/Restoral Report.

AC Tag Along

Default: Yes
Selections:
Yes Send AC messages as tag along events.

No Do not send AC messages as tag along events.

This parameter sends AC reports only if any other event occurs while AC is off-normal.
RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Tag Along.

AC/Battery Buzz

Default: No
Selections:
Yes Initiate panel-wide trouble tone at all keypads.

No Do not Initiate panel-wide trouble tone at keypads.

This parameter initiates a panel-wide trouble tone at keypads when the AC fails or the battery is low or missing.
This parameter does not prevent AC fail or low battery displays at the keypad.
RPS Menu Location
Panel Wide Parameters > Power Supervision > AC/Battery Buzz

Battery Fail/Restoral Report

Default: Yes
Selections:

Yes Battery failure and restoral reports are sent to the central station. They are routed to the telephone number programmed for *Power/Phone* events.

No Battery failure and restoral reports are NOT sent to the central station.

This parameter determines if a report is sent if the battery is low or missing.
The battery must be discharged below 12.1 VDC 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.

Modem reports Missing or shorted BATTERY MISSING; discharged below 12.1 VDC BATTERY LOW

Contact ID reports Missing or shorted BATTERY MISSING/DEAD; discharged below 12.1 VDC LOW SYSTEM BATTERY

RPS Menu Location
Panel Wide Parameters > Power Supervision > Battery Fail/Restoral Report.

3.10 RPS Parameters

RPS Passcode

Default: 999999
Selections: 6-24 characters
This parameter verifies that the RPS operator has valid access to connect to the control panel.
Enter 6-24 characters. Do not use SPACE in the passcode.
The control panel provides an RPS passcode configuration option. This option accepts up to 24 characters, but will allow shorter passcodes. The minimum passcode length is six characters and it is case sensitive. When RPS connects to the control panel, the correct passcode must be supplied before the control panel will allow RPS to access any configuration data or control functions.
The RPS passcode defaults to "999999" in the control panel. In an RPS default account, the passcode is also "999999". A default RPS account can connect to a default control panel without modifying the RPS passcode in either the RPS account or in the control panel.
RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Passcode

Log % Full

Default: 0
Selections: 0 to 99
0 (zero)- This setting 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.

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.
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.
RPS Menu Location
control panel Wide Parameters > RPS Parameters > Log % Full.

Contact RPS if Log % Full

Default: No
Selections: Yes/No
This parameter enables the control panel to automatically contact RPS when the “Log % Full” limit is reached.
RPS Menu Location
Panel Wide Parameters > RPS Parameters > Contact RPS if Log % Full.

RPS Call Back

Default: No
Selections:

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 Refer to RPS Phone #. 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.

IMPORTANT: When using the RPS Callback function, enter a "C" as the last digit in the RPS phone number if DTMF dialing is used.

This parameter 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.
RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Call Back

RPS Line Monitor

Default: Yes
Selections:

Yes This setting allows the control panel to communicate with RPS after the answering machine has answered the phone.

No Use this setting if the control panel is not sharing the phone line with an answering machine.

This parameter 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.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Line Monitor

Answer Armed

Default: 7
Selections:
0 (zero) This setting disables answering the phone.

1 to 15 (rings) Use this setting to have the control panel answer the phone after the specified number of rings when all areas are All On

IMPORTANT: RPS considers Part On as a disarmed state.

This parameter sets 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.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > Answer Armed

Answer Disarmed

Default: 7
Selections: 0 to 15 (rings)
0 (zero) This setting disables answering the phone.

1 to 15 (rings) Use this setting to have the control panel answer the phone after the specified number of rings when all areas are All On

IMPORTANT: RPS considers Part On as a disarmed state.

This parameter sets the telephone ring counter to answer when any area is in a Part On or disarmed state.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > Answer Disarmed

RPS Phone

Default: Blank
Selections: Up to 24 characters
This parameter specifies the phone number the control panel dials to contact RPS. The control panel dials the programmed number using RPS Phone # as a result of the following events:
- Log % Full threshold is achieved (if enabled).
- The control panel is contacted by RPS and RPS Call Back is programmed Yes
- User selects MENU > Actions > RPS > Call Via Phone (only one attempt is made).

If this parameter is left empty (blank), the control panel does not dial a phone number for RPS. Refer to Phone 1,2,3,4 when programming this parameter.

RPS Menu Location

Panel Wide Parameters > RPS Parameters > RPS Phone

RPS Modem Speed

Default: 1200
Selections: 300, 1200, 2400
This parameter sets the baud rate for RPS-to-control panel-communication when using a PSTN connection.
RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Modem Speed

3.11 Miscellaneous

Duress Type

Default: 0
Selections:
0 Disabled.

1 Increase the last digit by 1 to generate an alarm.
For example:
- If the passcode is 6123, 6124 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.

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: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **3**. Refer to SIA CP-01 Verification for more information.
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).
RPS Menu Location
Panel Wide Parameters > Miscellaneous > Duress Type.

Cancel Reports

Default: Yes
Selections:

Yes Send Cancel, Fire Cancel and Gas Cancel reports according to *Routing*.

No Do not send Cancel, Fire Cancel and Gas Cancel reports.

Use this parameter to determine whether or not Cancel, Fire Cancel and Gas Cancel reports are sent.

IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. Refer to SIA CP-01 Verification for more information.

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

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Cancel Reports

Call for Service Text- First Language

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, numbers and symbols.

- 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.

Note: First and Second languages are programmed during panel account setup in the Panel Data window. Supported languages include English, Spanish, French and Portuguese. To view the languages selected during account set-up, refer to Panel Wide Parameters > Personal Notification > User Language.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Call for Service Text - First Language

Call for Service Text - second language

Default: Blank
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 from the Latin-1 8-bit (ISO/IEC 8859-1) character set to describe the area.

- 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.

Note: First and Second languages are programmed during panel account setup in the Panel Data window. Supported languages include English, Spanish, French and Portuguese. To view the languages selected during account set-up, refer to Panel Wide Parameters > Personal Notification > User Language.

RPS Menu Location:

Panel Wide Parameters > Miscellaneous > Call for Service Text- Second Language

On-site Authorization for Firmware Update

Default: No
Selections:
Yes Require on-site authorization.

No On-site authorization is not required.

This parameter requires authorized on-site personnel to enter the authorization code at one of the keypads at the designated time during the remote firmware update process.
IMPORTANT Set this parameter to "Yes" for UL listed systems.
If authorization is required, you can modify the authority level required for the authorized user.
NOTE: It is recommend that a full system test be performed whenever firmware is updated locally or remotely.
Remote firmware updates through Remote Programming Software (RPS) using the RPS Firmware Update Wizard through the IP connection (on-board Ethernet connection, B426 Conettix Ethernet Communication Module, or B440 Conettix Plug-in Cellular Communicator), provides for easy feature enhancements without replacing ROM chips.
Remote firmware updates must be authorized on-site for UL listed systems.
RPS Menu Location:
Panel Wide Parameters > Miscellaneous > On-Site Authorization for Firmware Update.
Additional resources:
Remote Firmware Update

Enclosure Tamper Enable

Default: No
Selections:
Yes This setting enables the tamper input to generate a system trouble.

No No tamper events will be generated from the tamper input.

This parameter monitors the enclosure and processes an enclosure tamper event when the enclosure is opened.
Note**:** This function can only be set from RPS.
If the option is changed from Yes to No, an existing enclosure tamper event is cleared, but its restoral is not logged or reported.
If the option is changed from No to Yes, the tamper input is not processed until after the control panel detects that the tamper input is normal.
Tamper or tamper restoral is recognized if the event lasts for at least 250 milliseconds. When the control panel is powered up, or is re-starting for any reason, the tamper input is ignored until the control panel sees the tamper input become normal. (The installer closes the enclosure.) Once normal (closed), opening the enclosure might cause an enclosure tamper trouble.
When an enclosure tamper event is processed, it is indicated on the keypads' displays and the keypads sound a trouble tone. When the enclosure tamper has been restored, the control panel automatically removes the tampered enclosure message from the

keypads' displays and the trouble tone is silenced if no other trouble events exist. While an enclosure tamper is displayed at the keypad, the tamper event does not affect the arming or disarming process.
If installed and enabled, detects control panel door has been opened.
RPS Menu Location:
Panel Wide Parameters > Miscellaneous > Enclosure Tamper Enable

Fire Summary Sustain

Default: Yes
Selections:

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 silenced fire or gas points in the system are returned to normal.

This parameter provides a continuous alarm output to keep fire or gas strobes active after the fire or gas bell has stopped sounding.
RPS Menu Location:
Panel Wide Parameters > Miscellaneous > Fire Summary Sustain

Fire Supervision Event Type

Default: 2 (Fire Supervision Restoral)
Selections:

0 (Fire Trouble Restoral)	The control panel transmits a FIRE TROUBLE RESTORE when a Fire Supervision point restores to normal.
1 (Fire Alarm Restoral)	The control panel transmits a FIRE ALARM RESTORE when a Fire Supervision point restores to normal.
2 (Fire Supervision Restoral)	The control panel transmits a FIRE SUPERVISION RESTORE when a Fire Supervision point restores to normal.

This parameter determines how the control panel transmits a Fire Supervision Restoral event.
RPS Menu Location
Panel Wide Parameters > Miscellaneous > Fire Supervision Event Type

Fire Trouble Resound

Default: No Fire Trouble Resound
Selections:

No Fire Trouble Resound	Keypads will not re-sound the trouble tone.
Fire Trouble Resound @ 12:00 PM	Keypads will re-sound the trouble tone at 12:00 P.M. (noon) if any fire or gas 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 trouble tone at 12:00 A.M. (midnight) if any fire or gas point that falls within the scope

of a keypad is in an off-normal state.

This parameter determines if a fire or gas trouble event, although previously acknowledged and silenced at a keypad, will automatically resound the 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.
A user's passcode must have an authority level of 1 or greater in an area to silence troubles.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Fire Trouble Resound

Early Ambush Time

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

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Early Ambush Time

Second Ambush Code

Default: Unique
Selections:

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.

This parameter determines whether the same passcode can be used to start and end the Early Ambush process.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Second Ambush Code

Abort Window

Default: 30 sec
Selections: 15 to 45 (seconds) (1-sec increments)
Use this parameter to enter the number of seconds the control panel delays sending an alarm event to the central station from a point with the Alarm Event Abort feature enabled.

IMPORTANT:
- To meet UL requirements, the combined Entry Delay and Abort Window time must not exceed 60 sec.
- For SIA CP-01 Compliance, Abort Window is a required parameter.

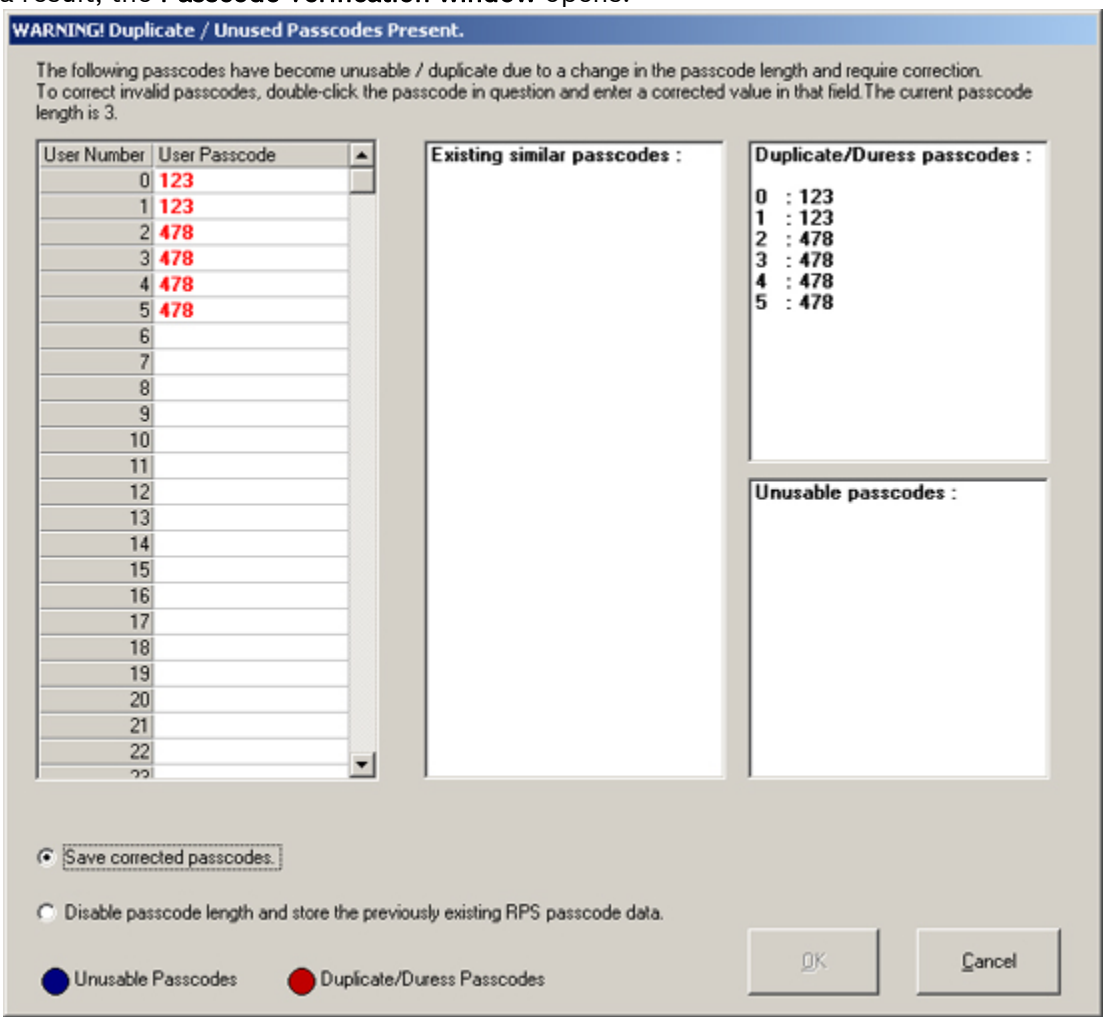
If an alarm silence operation is performed before this time elapses, the alarm transmission is aborted and the keypad shows an optional message (Refer to Abort Display).
When an abort alarm timer starts, it does not stop until an alarm silence operation is performed, or the time expires. This feature does not apply to fire alarms or invisible point alarms.

RPS Menu Location

Panel Wide Parameters > 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. Refer to SIA CP-01 Verification for more information.
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:
– Click the appropriate cell in the User Passcode column to select the passcode.
– Press the [Backspace] key on your keyboard to clear the cell.
– 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 control 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 control 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."

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Passcode Length

Swinger Bypass Count

Default: 2
Selections: 1 to 4
This parameter sets the maximum number of faults allowed on a point 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**. Refer to SIA CP-01 Verification for more information.
When upgrading a non-control panel account to a control panel account, RPS forces the default to **4**. Use this value for backward compatibility with previous control panel operation.
RPS Menu Location
Panel Wide Parameters > Miscellaneous > Swinger Bypass Count

Remote Warning

Default: No
Selections:

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, Inovonics Pendant Transmitter or key fob).
No	No remote warning occurs to annunciate the arming or disarming of an area through remote software, or a remote arming device (keyswitch, or key fob).

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**. Refer to SIA CP-01 Verification for more information.
When upgrading a non- control panel account to a control panel account, RPS forces the default to **No**.
RPS Menu Location
Panel Wide Parameters > Miscellaneous > Remote Warning

Crystal Time Adjust

Default: No
Selections:

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.

This parameter determines how the control panel regulates its clock time.
RPS Menu Location
Panel Wide Parameters > Miscellaneous > Crystal Time Adjust

Part On Output

Default: No
Selections:

Yes	The Fail to Close outputs become Part On outputs. This output is activated when all areas assigned to the same output are armed Part On Instant or Part On Delayed.

No The Fail to Close outputs operate when the closing window expires for the specified area.

This parameter activates outputs when all areas assigned to the same output are armed as Part On Instant or Part On Delay.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Part On Output

RPS Menu Location

Fail To Close

Early Area Armed Output

Default: No

Selections:

Yes Activates the area wide armed or Part On output at the start of Exit Delay time.

No Activates the area wide armed or Part On output at the end of Exit Delay time.

This parameter activates the area wide armed output

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Early Area Armed Output

Daylight Saving Time

Default: US Calendar

Selections:

US Calendar The control panel adjusts its clock for daylight saving time.

Disabled The control panel will not adjust its clock for daylight saving time.

This parameter enables the control panel to adjust its clock according to US daylight saving rules.

RPS Menu Location

Panel Wide Parameters > 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)

Time Zone
(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

Time Zone
(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

Time Zone
(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.
RPS Menu Location:
Panel Wide Parameters > Miscellaneous > Time Zone

3.12 Personal Notification

3.12.1 Personal Notification Destinations

Description

Default: Cell Phone User Name #
Selections: 0 to 24 characters in length
This parameter sets the text to identify the personal notification device or notification addressee. Text entered here is for reference only.
RPS Menu Location
Panel Wide Parameters > Personal Notification > Personal Notification Destinations > Description.

SMS Phone #/email address

Default: Blank
Selections: 0-255 characters
This parameter specifies either the destination phone number that will receive an SMS text notification or the email address that will receive an email message. The control panel sends personal notifications only if a B440 Conettix Plug-in Cellular Communicator is connected.

SMS Phone #
The control panel can send an SMS message to any mobile phone number, regardless of the cellular carrier. To configure SMS to SMS, enter the mobile phone number as the SMS Phone #, and set Method to “Plug-in Cellular SMS”
The B440 sends personal notifications to a cellular device when the programmed destination is a valid cellular telephone number containing only numbers 0-9. Properly interspersed hyphens are allowed, but not required.
– Starting with a 1 is optional.
– Use numbers only.
– Enter a maximum of 11 digits.

Email Address
The control panel can send emails to customer cell phones. All major cellular providers maintain an email-to-SMS bridge for this purpose.

IMPORTANT

The cellular provider's bridge will only send SMS messages to customers of that cellular provider's network. The installer must know the phone number and cellular carrier of the customer in order to use this feature.

The control panel can send an email notification directly to users' email addresses. This is the most cost-effective way to enable personal notifications. To configure Email to Email notifications, enter the email address of the user, and set the Method to "Plug-In Cellular Email" or "Onboard Ethernet Email". Be sure the email server configuration is correct, refer to Email Overview.

The B440/B441 sends personal notifications to email accounts when the programmed destination is a valid email address. An email address is considered valid if it is copied verbatim from an internet email provider. Use the @ character in this field if sending through a cellular module. This identifies the string as an email address.

Note: if the destination is neither a valid phone nor valid email, no message will be sent and an SMS send error will be logged. This is used to store the SMS phone number or an email address.

RPS Menu Location

Panel Wide Parameters > Personal Notification > Personal Notification Destinations > SMS Phone #/email address

User Language

Default: 1:(language programmed as first language in Panel Data window)

Selections: 1:(first language), 2:(second language)

This selection determines the language that the personal notification message is sent in.

First and Second languages are programmed during panel account setup in the New Panel Data window. Supported languages include English, Spanish, French and Portuguese.

RPS Menu Location

Panel Wide Parameters > Personal Notification > Personal Notifications Destinations > User Language

Method

Default: None

Selections:

None

Plug-in Cellular SMS	May be selected if you have a B440, B441, B442 or B443 plug-in cellular module.
Plug-in Cellular Email	May be selected if you have a B440, B441, B442 or B443 plug-in cellular module.
Bus Device Cellular SMS	May be selected if you have a B450 plug-in cellular module.
Bus Device Cellular Email	May be selected if you have a B450 plug-in cellular module.
Onboard Ethernet Email	May be selected if your connection is on-board IP.

This selection will determine if an SMS (text message) or email is sent to the desired Personal Notification destination and it determines which device will be used to route the message.

RPS Menu Location

Panel Wide Parameters > Personal Notification > Personal Notifications Destinations > Method

3.12.2 Personal Notification Reports

IMPORTANT CELLULAR SERVICE INFORMATION

Refer to Configuring for Cellular Communication for important information regarding how to set up your control panel to ensure proper cellular communication with the central station receiver.

Personal Notification 1-4

Default:

- Route Groups 1-3 0:Disabled
- Route Group 4 1, 2, 3, 4

Selections: 1-16

This parameter can be set to send personal notifications to a cellular device or email address.

The control panel sends personal notifications only if a B440 Conettix Plug-in Cellular Communicator is connected. The B440 sends personal notifications to a cellular device when the programmed destination is a valid cellular telephone number containing only numbers 0-9. Properly interspersed hyphens are allowed, but not required.

The B440 sends personal notifications to email accounts when the programmed destination is a valid email address. An email address is considered valid if it is copied verbatim from an internet email provider.

Note:

- If the destination is neither a valid phone or valid email, no message will be sent, and an SMS send error will be logged.
- You are not required to set the Primary or Backup Path Device parameters to Cellular IP for Personal Notification by SMS to work.

RPS Menu Location:

Panel Wide Parameters > Personal Notification > Personal Notifications Reports > Personal Notification 1-4

Personal Notification Attempts

Default: 3

Selections: 1-6

This parameter sets the maximum number of attempts the control panel makes to send a personal notification.

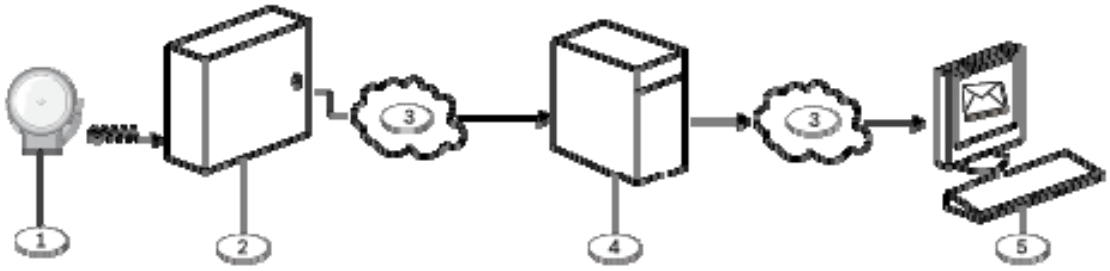
RPS Menu Location:

Panel Wide Parameters > Personal Notification > Personal Notification Attempts

3.12.3 Email Server Configuration

Email Overview

The B Series control panels v2.01 and higher can be programmed to send personal notifications to one or more email addresses.
When an event occurs, the control panel creates a report and transmits it as data strings across an IP network to an email server. The SMTP (Simple Mail Transfer Protocol) email server translates the strings into text and then pushes it out to up to 16 destinations as programmed under Personal Notifications Destinations. This is a one-way communication from the panel to the user.



Callout - Description	Callout - Description
1 - Alarm event	4 - SMTP email server
2 - Compatible Bosch control panel	5 - Computer or other device used to receive email
3 - Internet	

SMTP Email Servers

SMTP email servers transfer messages to personal notification email addressees. The address associated with the SMTP email server you choose is programmed into RPS in the Email Server Name/Address parameter. For all public email providers, the SMTP server information is available on the internet. Refer to the table below for a sample of some common server configurations. If you can't locate the address for your SMTP email server, contact your email provider.

Provider	SMTP Server URL	Port	Authentication/Encryption
Gmail	smtp.gmail.com	465	Encrypted
Yahoo (unencrypted)	smtp.mail.yahoo.com	25	Authenticate
Yahoo (encrypted)	smtp.mail.yahoo.com	465	Encrypted
Verizon	smtp.verizon.net	465	Encrypted
AT&T	outbound.att.net	465	Encrypted
Comcast	smtp.comcast.net	465	Encrypted
Time Warner	smtp-server.<region>.rr.com	25	Authenticate

Setting up an Email Account

To setup an email account that provides emails to the Personal Notification destinations, register for an email account from any of the email providers such as those listed in the table above. Choose a user name that will make it easy for individuals receiving notifications to identify emails coming from the control panel (example: panelaccountxyz). The user name and password you specify when registering for this account is the Authentication User Name and Authentication Password you will need to program into RPS (example: panelaccountxyz@gmail.com).

Email Server Name/Address

Default: Blank
Selections: Blank, 0-255 ASCII printable characters
This parameter specifies either the name or the address of the SMTP (Simple Mail Transfer Protocol) for the email server chosen to transfer event messages from the control panel to a designated email address. (Example: smtp.gmail.com)
RPS Menu Location
Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Name/Address
Additional Information
Email Overview
Email Server Port Number
Email Server Authentication/Encryption
Authentication User Name
Authentication Password

Email Server Port Number

Default: 25
Selections: 1-65535
This parameter specifies the port number for the email server.
Port 25 is the default SMTP port for most outgoing servers. If the IP denies the default port number (generally because of the massive spam and malware traffic), try another commonly used port such as **port 587** or **port 465** to avoid the block.
RPS Menu Location
Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Port Number
Additional Information
Email Overview
Email Server Name/Address
Email Server Authentication/Encryption
Authentication User Name
Authentication Password

Email Server Authentication/Encryption

Default: Authenticate
Selections:

Basic	No authentication, no encryption
Authenticate	Authentication required, no encryption

Encrypted Authentication required, encryption required

Use this parameter to set the security level required by the email server to receive messages from the control panel.
Authentication means that the email server requires an authentication username and authentication password. This is sometimes referred to as SMTP-AUTH.
The Encryption used is Transport Layer Security (TLS)

RPS Menu Location

Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Authentication/Encryption

Additional Information

Email Overview
Email Server Name/Address
Email Server Port Number
Authentication User Name
Authentication Password

Authentication User Name

Default: Blank
Selections: Blank, 0-255 ASCII printable characters
This parameter specifies the user name for the email account that is set up to receive messages from the SMPT server sent by the control panel.

RPS Menu Location

Panel Wide Parameters > Personal Notification > Email Server Configuration > Authentication User Name

Additional Information

Email Overview
Email Server Name/Address
Email Server Port Number
Email Server Authentication/Encryption
Authentication Password

Authentication Password

Default: Blank
Selections: Blank, 0-49 ASCII printable characters
This parameter sets the password that the SMPT server uses to send emails to the Personal Notification destinations.

RPS Menu Location

Panel Wide Parameters > Personal Notification > Email Server Configuration > Authentication Password

Additional Information

Email Overview
Email Server Name/Address
Email Server Port Number
Email Server Authentication/Encryption
Authentication User Name

4 Area Wide Parameters

4.1 Area/Bell Parameters, Open/Close Options

Area Overview

Definition
An area is defined as a geographically grouped set of points.

Configurations
Area programming offers a wide selection of different system configurations. The control panel assigns an account number to each area to define annunciation, control, and reporting functions. Make area arming conditional on other areas (master or associate), if desired. You can configure any area for perimeter and interior arming, not requiring a separate area for this function. Link multiple areas to a shared area which is automatically controlled (hallway or lobby).

IMPORTANT Linking multiple areas only applies to B5512 control panels.

For systems with more than one area, all areas must be under the responsibility of one ownership and management. This may be a group of buildings attached or unattached and may even have different addresses but are under the responsibility of someone having mutual interest (other than the alarm installing company). This does not apply to strip mall applications where each independent business must have their own separate alarm system.
An example for a commercial system would be a business that has an OFFICE area and a WAREHOUSE area in a building where each area can be armed or disarmed independently.
As a residential example a system could be configured with the garage and house as separate areas.
In each of the examples above all of the areas are under the sole responsibility of a single owner.
In multi-area systems the bell (or siren) and control panel must be in one of the protected areas.
The bell or siren must be located where it can be heard by users who turn areas on and off (arm and disarm).

Area On

Default:
B5512:
– Area 1: Yes
– Areas 2-4: No
B4512:
– Area 1: Yes
– Areas 2: No
B3512:
– Area 1: Yes
Selections: Yes/No
Yes Area is enabled.

No Area is disabled.
This parameter enables or disables the specified area.
When an area is set to No:
– 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.
The B5512 supports up to 4 areas, the B4512 supports 2 areas, and the B3512 supports 1 area.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area On

Account Number

Default: 0000
Selections: 4 or 10 digit numbers, 0-9, B-F
This parameter determines the account number reported for this area. An account number must be assigned to each active area.
If 5 or more digits are used in the account number, RPS automatically pads the number with leading zeros to make it a ten-digit number.
CAUTION:
– Make sure the central station automation software is compatible with 10-digit account numbers before programming a 10-digit account number into the control panel.
– Account numbers must not include 'A' for any digit.
Account numbers are used to group areas together. Each area can have a different account number, or several areas might share the same account number. The control panel uses the account number as a reference for arming and keypad text displays.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Account Number.

Force Arm/Bypass Max

Default: 2
Selections:
B5512: 0-16
B4512: 0-10
B3512: 0-10
This parameter specifies the maximum number of combined controlled points that can be faulted or in a bypassed state when arming this area.
Refer to Force Arm Returnable and Bypass Arm 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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Force Arm/Bypass Max.

Delay Restorals

Default: No
Selections:
Yes Point restoral events are not logged or reported until the point has physically restored and the bell silenced.
No Point restoral events are logged and reported when the point physically restores.
Use this parameter to delay restoral reports until bell time expires.
For Fire/Gas Alarm/Supervisory points, restoral events are not logged or reported until the point has physically restored, the bell silenced, and the event cleared from the keypads.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Delay Restorals.

Exit Tone

Default: Yes
Selections:
Yes Sound an exit tone at all keypads during exit delay.
No Turn off exit tones for individual keypads (based on their KP# 1 through 8).
This parameter sounds an exit tone during exit delay at all keypads assigned to this area.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Tone.

Exit Delay Time

Default: 300
Selections: 0 to 600 (seconds) (in 5 second increments)
This parameter sets the exit delay time for this area when All On, Exit or Part On, Exit arming is used.
Points programmed for instant alarms generate alarms immediately, even during exit delay.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter between 45 and 255 seconds. Refer to SIA CP-01 Verification for more information.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Time.

Auto Watch

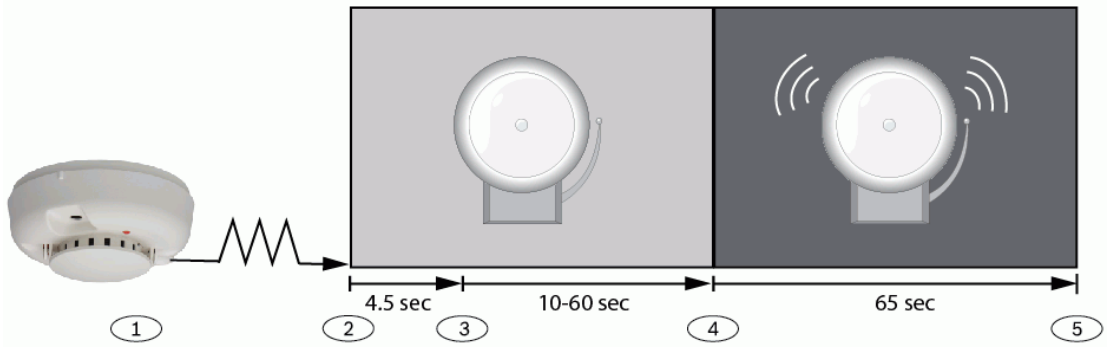
Default: No
Selections:
Yes When the area is disarmed, Watch Mode is turned on automatically.
No When the area is disarmed, Watch Mode must be turned on or off manually.
Use this parameter to automatically put the area in Watch Mode when the control panel is disarmed.
Controlled points programmed as 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. Perimeter points still report as alarms or troubles.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Watch.

Restart 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 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:
- 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 to 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. Restart 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.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Restart Time.

Duress Enable

Default: No
Selections:
Yes Enable Duress alarm for this area.
No Disable Duress alarm for this area.
This parameter determines if this area allows duress alarms to be generated.
IMPORTANT: To comply with SIA CP-01, set this parameter to **Yes**.
If [MENU 35] 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. 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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Duress Enable

Additional resources
Refer to Duress Type for an explanation of Duress.

Area Type

Default: Regular
Selections:
B5512
– Regular
– Master
– Associate
– Shared
B4512 and B3512
– Regular

Regular	Arms or disarms as an independent area.
Master	Does not allow arming for this area unless all Associate areas with the same A# Acct Number are exit delay arming or are All On Delay. A Check Area message 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	Allows 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. 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. 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, Sked or by the RPS. The scope of all Associate areas must include the Shared area(s) in order to view faulted points. Shared areas: Are not associated to other areas by account number, they are shared panel wide. Are armed when all Associate areas in the control panel are put into All On Delay state. Are disarmed when at least one Associate area in the control panel is taken out of All On Delay state. ***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.

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 cannot be armed by passcode, keyswitch 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 control panel is disarmed. Shared areas cannot be disarmed by passcode, cards, keyswitch 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] displays 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 force arms the Shared area if: the user has authority to bypass points, the point is bypassable, AND the number of faulted points does not exceed the force arm 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 restarts and allow a user to walk to an Associate area and disarm. If the 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 disarms when the 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 B5512 supports up to 4 areas, the B4512 supports up to 2 areas, and the B3512 supports 1 area.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Type.

Two Man Rule?

Default: No

Selections:

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.

This parameter sets the requirement for two valid passcodes to be entered on the same keypad to disarm the area.

IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **No** for all enabled areas. Refer to SIA CP-01 Verification for more information.

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 event occurs if entry delay ends before the second valid passcode is entered.

If the area is already in an alarm event, 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.

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.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Two Man Rule

Early Ambush?

Default: No

Selections:

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.

This parameter requires two valid passcodes to disarm the area within the time limit set in the Early Ambush Time parameter.

IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **No** for all enabled areas. Refer to SIA CP-01 Verification for more information.

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 an All On area, or during the entry delay period for All On.
You can create a custom function that will disarm the area using passcode disarm. 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.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Early Ambush

Fire Time

Default: 6
Selections: 1 to 90 (minutes) (in one minute increments)
This parameter sets the length of time in minutes the bell rings for fire alarm points.

IMPORTANT: Check with your Authority Having Jurisdiction (AHJ) to determine the appropriate bell time for your geographical area.

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. Set this parameter for two minutes or more to ensure you have ample output time.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fire Time

Fire Pattern

Default: Pulsed
Selections:

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.)

This parameter selects 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.

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)
This parameter sets the number of minutes the bell rings for burglary alarm points.

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. Refer to SIA CP-01 Verification for more information.

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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Burg Time.

Burg Pattern

Default: Steady
Selections:

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.)

Select the bell pattern this area uses to signal an alarm on a non-fire point.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Burg Pattern

Gas Pattern

Default: Temporal Code 4
Selections:

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.

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.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Gas Pattern

Single Ring

Default: No

Selections:

Yes This setting produces one bell output per arming period. After one alarm, alarms on non-fire points in the same area cannot restart the bell until the armed state changes.

No Restart bell output with each alarm event.

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.

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.

This parameter does not silence the keypad alarm bell tone or prevent any reports. Fire points are not affected and bell time is restarted with each new alarm.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Single Ring.

Bell Test

Default: No

Selections:

Yes Initiate bell test.

No Do not initiate bell test.

This parameter provides an alarm output from the output programmed at Alarm Bell after the closing report has been confirmed or the exit delay time has expired.

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.

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.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Bell Test

Account O/C

Default: No

Selections:

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.

No Do not send opening and closing reports by account.

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.

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.

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.

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

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Account O/C

Area O/C

Default: Yes

Selections:

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.

This parameter determines if the area number and the account number are sent upon arming and disarming.

As long as Acct O/C is set to No, the account number is sent when arming this area individually. If 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).

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 Arm:** Part On Open/Close = E

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area O/C

Disable O/C in Window

Default: Yes

Selections:

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. Refer to 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.

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 and printed on a local printer, if installed.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Disable O/C in Window

Auto Close

Default: No

Selections:

Yes The area automatically arms All On Delay 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.

With this parameter, the control panel can automatically arm the area All On Delay at the end of the closing window regardless of the previous armed state.
Regardless of Force Arm/Bypassable Max or Bypassable, an unconditional force arm occurs resulting in faulted points being left out of the system. Refer to Force Arm Returnable or Bypass Returnable for details on returning these points to service.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Close

Fail To Open

Default: No
Selections:
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.
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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fail To Open

Fail To Close

Default: No
Selections:
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.
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.
An exit delay time must be programmed in Exit Dly Time.
If Auto Close is set to Yes, a report is sent because it occurs when the closing window stop time occurs.
If Disable O/C in Window is set to Yes, Fail to Close report is followed by Closing Late or Force Close Late report.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fail To Close

Latest Close Time

Default: Disabled
Selections:
Disabled RPS sends 0:00 to the control panel.

00:30 to 23:30 Set the time for latest close. Set in 30 minute increments using 01 to 24 to specify the hour.
Midnight RPS sends 24:00 to the control panel.

Use this parameter to set a latest close time boundary when an open/close window is assigned to the selected area.
If the Latest 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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Latest Close Time

Restricted O/C

Default: No
Selections:
Yes Restrict opening and closing reports for this area. Area O/C must be set to Yes to generate restricted opening and closing reports.
No Do not restrict opening and closing reports for this area. Regardless of programming in Restricted O/C , reports are not restricted in this area when this item is set to No.
This parameter determines if this area can restrict opening and closing report activity. Was Force Armed and Forced Close events are still sent to the central station if enabled in routing when force arming the system.
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.
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 was 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 does 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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Restricted O/C

Part On O/C

Default: No
Selections:
Yes This area can send Part On opening and closing reports.
No This area cannot send Part On opening and closing reports.
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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Part On O/C

Exit Delay Restart

Default: Yes
Selections:
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.
This parameter activates when a controlled point with delay alarm response changes from normal to faulted and back to normal, then faulted again 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.
RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Restart

All On - No Exit

Default: Yes
Selections:
Yes Switch the arming state of the area from All On Delay to Part On Delay.
No Keep the arming state of the area All On Delay.
This parameter selects whether or not the arming state for an area changes from All On to Part On if no perimeter 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.
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.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > All On - No Exit

Exit Delay Warning

Default: No
Selections:
Yes Pulse the alarm output for the last 10 seconds of Exit Delay
No Do not pulse the alarm output during Exit Delay
This parameter enables the alarm bell to pulse on and off every two seconds for the remaining 10 seconds of Exit Delay.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Yes**. Refer to SIA CP-01 Verification for more information.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Delay Warning

Entry Delay Warning

Default: No
Selections:
Yes Pulse the alarm output for the last 10 seconds of Entry Delay
No Do not pulse the alarm output during Entry Delay
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**. Refer to SIA CP-01 Verification for more information.
When upgrading a non-control panel account to a control panel account, RPS forces the default to **No**.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > 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 delays until it rearms to All On Delay.
The area automatically rearms at 11:59 pm 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 set to 4 hours and the area is disarmed at 10:30 pm, the area rearms at 11:59 pm (1 hour and 29 minutes after disarm).
IMPORTANT
Force Arm / Bypass Max is ignored when rearming.
Users can use Extend Close to lengthen an active rearm delay.
RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Re-Arm Time

4.2 Area Names

Area Name Text

Default: Area # (# = the Area number)
Selections: Up to 32 characters
This parameter sets what is displayed at keypads. This is for informational purposes only.
Enter up to 32 characters of text, numbers and symbols to describe the area.
- Keypads display the first 20 characters. If more than 20 characters are used, the area name 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.

The B5512 supports up to 4 areas. The B4512 supports up to 2 areas. The B3512 supports 1 area.
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 2-8 = 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 (for all KP addresses)

Selections:
- **B5512**: 1 to 4
- **B4512**: 1 to 2
- **B3512**: 1

This parameter assigns the keypad to an area.

The B5512 supports up to 4 areas, the B4512 supports up to 2 areas, and the B3512 supports 1 area.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Area Assignment

Keypad Language

Default: First Language, follow User language (for all KP addresses)

Selections:
- First Language, follow User Language
- First Language, ignore User Language
- Second Language, follow User language
- Second Language, ignore User language

This parameter sets the language that is displayed at the keypad.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Keypad Language

Scope

Default:
- Address 1: Panel Wide
- Addresses 2-8: Area Wide

Selections:

B5512
- Area Wide
- Account Wide
- Panel Wide
- Custom

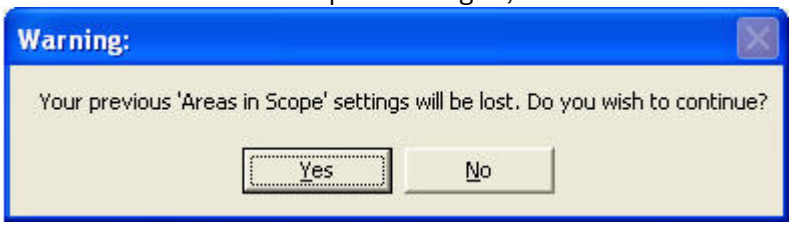
B4512
- Area Wide
- Panel Wide

B3512
- Area Wide
- Panel Wide

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 it is assigned to.
Account Wide	n account keypad can view information, and perform arming and disarming functions for all areas that have the same account 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.This is normally used with a Master area.
Custom	A custom keypad can select Areas in Scope.

Whenever the custom 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 Areas in Scope parameter in the B4512 is automatically set according to the option selected in this parameter.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Scope

Additional resources

Acct Number
Area Type
Areas in Scope

Areas In Scope

Default:
– Address 1: All
– Addresses 2-8: 1

Selections:
– B5512: All, 1, Dbl click to view
– B4512: All, 1
– B3512: 1

All All areas within the scope of this keypad are affected.
1 Only area 1 is affected.
Dbl click to view Areas included within the scope of the keypad have been custom selected. Double click to view or select custom areas.
This parameter identifies the areas included in the scope of this keypad for viewing status, arming or disarming.
Custom Areas in Scope apply to B5512 only. The options in this parameter are automatically set in the B4512 according to the option selected in Scope and cannot be changed.
The B5512 supports up to 4 areas. The B4512 supports up to 2 areas. The B3512 supports 1 area.

RPS Menu Location
Keypads > SDI2 Keypad Assignments > Areas in Scope

Additional resources
Scope

Passcode Follows Scope?

Default: Yes
Selections: Yes/No

Yes User can change the armed state of all areas within the scope of that keypad. User can turn the area on or off by using Passcode +[ENTER],a keyfob, or a credential. User can change the armed state of all areas within the scope of that keypad. User can turn the area on or off by using Passcode +[ENTER],a keyfob, or a credential.

No User can change the armed state of the area that the keypad is assigned to. User can turn the area on or off by using Passcode +[ENTER],a keyfob, or a credential.

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. Users can turn the area On or Off using Passcode + [ENTER], a keyfob, a credential, or by using the keypad's On/Off menu.
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. Users must have authority enabled in Passcode Arm and Passcode Disarm.

RPS Menu Location
Keypads > SDI2 Keypad Assignments > Passcode Follows Scope

Additional resources
Scope

Area Assignment
Passcode Arm
Passcode Disarm

Enter Key Output

Default: 0 (for all KP addresses)
Selections:
- **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- **B4512:** 1(A), 2(B) or 3(C), 0, 11-18, 21-28, 31-38
- **B3512:** 1(A), 2(B) or 3(C), 0

0	The [ENTER] key does not cycle an output.
1 to 58	Assigned number that cycles an output when Passcode Enter function is used.
A(1), B(2), C(3)	Assigned onboard output that cycles when Passcode Enter function is used.

This parameter assigns an output number or letter that momentarily activates when the [Enter] key is pressed at this keypad after the user enters a valid passcode.

IMPORTANT: Passcode Enter Function cannot be set to "Cycle Output" unless this parameter is set to a value other than “0”.

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 an 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.

This parameter can be used to provide a low-level access control strike on a door. It does not shunt a point.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Enter Key Output

Additional resources

Passcode Enter Function

Passcode Enter Function

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

Arm/Disarm	Passcode + [ENTER] starts All On Delay arming for all areas within the users scope if the current area is disarmed. If the area is not disarmed (off), then all areas in scope are disarmed.
Cycle Output	Passcode + [ENTER] key activates Enter Key Output for 10 seconds.
Auto Re-Arm	If the area assigned to the keypad is armed All On Delay, passcode + [ENTER] starts Exit Delay. If the areas is Off, passcode + [ENTER] does not arm, the area remains off.
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 parameter defines a single purpose to this keypad; however entering a passcode with authority in the keypad's area always silences alarms and troubles.
When a Passcode Enter Function is unable to be executed due to configuration conflicts, the control panel performs the Arm/Disarm function regardless of setting.
The Service Passcode (User ID 0) does not follow the Passcode Enter Functions.
When configuring the control panel, do not share with any other point, sensor reset, control panel, or bell functions. Outputs used for the Cycle Output function. Sharing can cause errors in output operation.

IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, keep this parameter at its default setting (Arm/Disarm).

RPS Menu Location
Keypads > SDI2 Keypad Assignments > Passcode Enter Function.

Dual Authentication

Default: No
Selections: Yes / No
This parameter sets the requirement that a user must present any two forms of authorization (passcode, credential or keyfob) at the keypad in order to gain access.
RPS Menu Location
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 first and second form of authorization (passcode, credential or keyfob).
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Dual Authentication Duration

Trouble Tone

Default: No (for all KP addresses)
Selections: Yes/No
Yes Panel wide trouble tones sound and visual displays show at this keypad.
No Panel wide troubles do not sound. Visual displays still show.
This parameter determines whether this keypad or any keypad with the same address setting, sounds the panel wide trouble tones.
Panel wide trouble tones include power, phone, SDI2 bus and bus. They do not include point troubles, or buzz on fault.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Trouble Tone.

Entry Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
Yes This keypad sounds entry tones.

No This keypad does not sound entry tones.
This parameter determines whether this keypad or any keypad with the same address setting sounds the 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 Entry Tone Off in Point Index.
Assign two keypads to the same area to have one sound the tone while the other does not.
Set this parameter to Yes for UL installations.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Entry Tone.

Additional Resource
Entry Tone Off

Exit Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
Yes This keypad sounds exit tones.
No This keypad does not sound exit tones.
This parameter determines whether this keypad or any keypad with the same address setting sounds the exit delay tone during the delay arming of an areas.
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 Exit Tone in Area Parameters.
Assign two keypads to the same area to have one sound the tone while the other does not.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Exit Tone

Arm Area Warning Tone

Default: Yes (for all KP addresses)
Selections: Yes/No
Yes This keypad activates a tone and warning display.
No This keypad does not activate a tone or warning display.
Use this parameter to determine whether this keypad sounds an audible tone and displays a warning on the keypad when a closing window has activated.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Arm Area Warning Tone.

Function Lock

Default: No (for all KP addresses)
Selections: Yes, No
Yes Pressing the Bypass, Menu, or Shortcuts key requires a passcode before proceeding.
No Pressing the Bypass, Menu, or Shortcuts key does not require a passcode until a function requiring one is selected.
This parameter determines if the Function Lock requires a passcode when pressed to access the functions.

The user is prompted to enter a passcode after pressing the Bypass, Menu, or Shortcuts 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 Bypass, Menu, or Shortcuts 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
Yes This keypad displays a message for all aborted alarms within its scope.
No This keypad does not display a message for aborted alarms within its scope.
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.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Abort Display

Cancel Display

Default: Yes (for all KP addresses)
Selections: Yes or No
Yes This keypad displays a message for all canceled alarms within its scope.
No This keypad does not display a message for canceled alarms within its scope.
Select whether or not the keypad displays a message 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**. When upgrading a non-control panel account to a control panel account, RPS forces the default to **No**.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Cancel Display.

Additional Resource
Cancel Reports

Nightlight Enable

Default: No (for all KP addresses)
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 (for all KP addresses)
Selections: Yes/No
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.
This parameter enables or disables the keypress acknowledgement tone on the keypad.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Silence Keypress Tone.

Show Date and Time

Default: No (for all KP addresses)
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
Additional Information
Change Keypad Display

Keypad Volume

Default: 7 (for all KP addresses)
Selections:

0 No keypress tone.

1-6

7 Maximum volume setting.

This parameter sets the volume level for the keypress acknowledgement tone on the keypad.
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: 0-6
0 = dimmest setting
6 = brightest setting
This parameter sets the brightness level for the LED display on the keypad. Keypad brightness can also be set at 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

Feature Button Option

Default: Language
Selections:

Language	Allows the user to switch between the first and second languages as configured under the Panel Info tab of the Panel Data dialog box.
Event Memory	Allows the user to quickly access and view Event Memory

This parameter sets which feature is displayed in the upper left corner of the status bar of the B942. This parameter applies to the B942.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Feature Button Option

5.2 Global Keypad Settings

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 > Global Keypad Settings > A Key Response

A Key Custom Function

Default: Disabled
Selections:
- **B5512:** Disabled, CF 128, CF 129, CF130, CF 131
- **B4512:** Disabled, CF 128, CF 129
- **B3512:** Disabled, CF 128

This parameter specifies the custom function that is run when the A Key on a B92x Two-line 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 > Global Keypad Settings > 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 > Global Keypad Settings > B Key Response

B Key Custom Function

Default: Disabled
Selections:
- **B5512:** Disabled, CF 128, CF 129, CF130, CF 131
- **B4512:** Disabled, CF 128, CF 129
- **B4512:** Disabled, CF 128

This parameter specifies the custom function that is run when the B Key on a B92x Two-line 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 > Global Keypad Settings > 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 > Global Keypad Settings > C Key Response

C Key Custom Function

Default: Disabled
Selections:
- **B5512:** Disabled, CF 128, CF 129, CF130, CF 131
- **B4512:** Disabled, CF 128, CF 129
- **B3512:** Disabled, CF128

This parameter specifies the custom function that is run when the C Key on a B92x Two-line 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 > Global Keypad Settings > C Key Custom Function

Manual Silent Alarm Audible on Comm Trouble

Default: No
Selections: Yes/No
Yes Enable the Alarm Bell to activate when the silent alarm event fails to reach central station.
No Disables the Alarm Bell from activating when the silent alarm fails to reach central station.
This parameter enables the Alarm Bell output to activate for the remaining Burg Bell time if a keypad or RADION keyfob silent alarm fails in two attempts to transmit its report to the configured destination.
The Alarm Bell outputs activated are the same outputs that would have been activated if the keypad or RADION keyfob alarm had been configured as a panic alarm. The bell timer was started when the silent alarm was generated so the Alarm Bell is only active for the configured Burg Time minus the time it took to attempt to report twice.
This option only has an effect if a keypad's C key or a RADION keyfob panic is configured to create a silent alarm.
RPS Menu Location
Keypads > Global Keypad Settings > Manual Silent Alarm Audible on Comm Trouble

Card Type

Default: 26 bit
Selections:
26 bit Site Code will be set to 255.
37 bit Site Code will be set to 0.
This parameter specifies the card format used.
IMPORTANT
Changing this parameter returns all entries currently under Card Data and Site Code to factory defaults for all the users.
RPS Menu Location
Keypads > SDI2 Keypad Assignments > Card Type

5.3 Global Wireless Keyfob Settings

Keyfob Function A Custom Function

Default: Disabled
Selections:
– **B5512:** Disabled, CF 128, CF 129, CF130, CF 131
– **B4512:** Disabled, CF 128, CF 129
– **B3512:** Disabled, CF 128
This parameter specifies the custom function that is run when the Auxiliary Function A button is pressed on the RADION keyfob.
On the RADION four-button keyfobs, pressing the third button activates Auxiliary Function A. When the auxiliary function button is pressed, the control panel performs the custom function configured in this parameter. If it is configured as disabled, then no action occurs.
RPS Menu Location
Keypads > Global Wireless Keyfob > Keyfob Function A Custom Function

Keyfob Function B Custom Function

Default: Disabled
Selections:
– **B5512:** Disabled, CF 128, CF 129, CF130, CF 131
– **B4512:** Disabled, CF 128, CF 129
– **B3512:** Disabled, CF 128
This parameter specifies the custom function that is run when the Auxiliary Function B button is pressed on the keyfob.
On the RADION four-button keyfobs, pressing the fourth button activates Auxiliary Function B. When the auxiliary function button is pressed, the control panel performs the custom function configured in this parameter. If it is configured as disabled, then no action occurs.
RPS Menu Location
Keypads > Global Wireless Keyfob > Keyfob Function B Custom Function

Keyfob Panic Options

Default: Panic response disabled
Selections:
– Panic response disabled
– Audible panic response enabled
– Silent panic response enabled
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.

RPS Menu Location

Keypads > Wireless keyfob > keyfob Panic Options.

6 Custom Function

Custom Functions -- Overview

Each Custom Function ### item has an 18 character programmable text. When the custom function is assigned to the Shortcut Menu Function the user can use 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 128-131 in the User Configuration section, to be capable of using the custom function.
The B5512 supports 4 custom functions, the B4512 supports 2 custom functions, and the B3512 supports 1 custom function.

Custom Function Text

Default:
- **B5512:** Function 128, Function 129, Function 130, Function 131
- **B4512:** Function 128, Function 129
- **B3512:** Function 128

Selections:
This parameter sets the menu text displayed at the keypad for the Custom Function item.
Enter up to 32 characters of text, numbers and symbols.
- 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.

RPS Menu Location
Custom Function > Custom Function Text.

Custom Function Text- second language

Default: Blank
Selections:
This parameter sets the menu text displayed at the keypad for the Custom Function item when the user is configured to use the Second Language text.
Enter up to 32 characters from the Latin-1 8-bit (ISO/IEC 8859-1) character set 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.

RPS Menu Location
Custom Function > Custom Function Text (Second Language)

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 "All On Delay" 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 "All On Instant" 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 "Part On Delay" 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 "Part On Instant" 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.

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. This auto-answer period will last for 2 minutes and overrides the Answer RPS Over Network? and RPS Address Verification prompt settings.

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 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 Report 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 Parameter 1: Deferred 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.

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.

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 #. Note: When using the Show Date & Time function with the Set Keypad Volume or Set Keypad Brightness functions in the same custom function they must be separated by about 10 seconds with the Delay function.

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 #.

RPS Menu Location

Custom Function > Function 1-6

7 Shortcut Menu

Function

Default:
- Shortcut Menu Item 1: All On Selected Area
- Shortcut Menu Item 2: Off Select Area
- Shortcut Menu Item 3: View Point Status
- Shortcut Menu Item 4: Reset Sensors
- Shortcut Menu Item 5: Change Watch Mode
- Shortcut Menu Item 6: Keypad Brightness
- Shortcut Menu Item 7: Keypad Volume
- Shortcut Menu Item 8: View Log
- Shortcut Menu Item 9-32: Disabled Item

Selections: Refer to list below.
This parameter assigns functions to menu items.
Select the function from the drop down list in the dialogue box that appears when you double-click a cell in the Function column and next to the function in the User Configuration section.
All supported custom functions are listed by their configured Custom Function Text.
There is no restriction on how many times you might assign a specific function to the menu. By doing so, you can assign the same function at different keypads so they appear in a different order in some areas than they would in others.

Function	Function	Function	Function
Disabled Item	View Point Status	RPS via Phone	Keypad Brightness
All On Delay	Send Status Report	Go to Area	Keypad Nightlight
All On Instant	Reset Sensors	Update Firmware	Keypad Volume
All On Select Area	Change OUTPUT State	View Service Bypassed	Silence Key Tone
Part On Delay	Fire Walk Test	Change Passcode	View Event Memory
Part On Instant	Intrusion Walk Test	Add User	Delete Event Memory
Part On Select Area	Service Walk Test	Edit User	View Log
Off	Invisible Walk Test	Delete User	A Key Alarm (Fire)
Off Select Area	Send Test Report	Change Watch Mode	B Key Alarm (Medical)
Extend Close	Display Revisions	Set Panel Date	C Key Alarm (Silent/Panic)
Bypass a Point	RPS Answer	Set Panel Time	CF 128
Unbypass a Point	RPS via Network	Show Date/Time	CF 129
View Area Status	RPS via Network, Change Port	Change Skeds	CF 130
			CF131

RPS Menu Location
Shortcut Menu > Function

Set/Clear All

Default: Set/Clear All
Selections: Address 1-8
Use this parameter to quickly enable or disable a selected function number at all available addresses.

Any changes you make in the **Set/Clear All** window also appear in the specific keypad Address # cell. For example, if you check the boxes for Address 1 and Address 2 in the **Set/Clear All Address** window, the cells for Address 1 and Address 2 change to show **Yes**. Likewise, if you change any of the Address # cells individually, those changes appear in the **Set/Clear All Address** window.

RPS Menu Location

Shortcut Menu > Set/Clear All

Address 1-8

Default:

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

Selections: Yes/No

Yes: This menu item appears at this keypad address.

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

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

RPS Menu Location

Function List > Address

8 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 control panel summary of alarms, troubles and supervisory events.
- 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 events such as a force arm have occurred.
- On-board Outputs: There are 2 on-board 12 VDC voltage-outputs which provide power when activated on the control panel. These outputs are default programmed from the factory as outputs A(1), B(2) and C(3). Typically, output A(1) is used for the Bell, output B(2) is used for an alternate alarm output (such as another bell) and output C(3) is used for Sensor Reset.
- Off-board Outputs: The control panel can also control as many as 40 dry contact form "C" outputs for the B5512 or 24 for the B4512 when up to 5 optional B308 OctoOutput Modules are installed. These outputs are used for Area Output, Panel Wide Output, and Individual Point Fault Outputs. (The B3512 does not support off-board points.)

Output Follows Point

Outputs can also be used to activate when a point programmed for, Output Response Type (in the point index section), is off normal or in alarm event.

Output Reports

When output activity is reported to the receiver (Refer to Routing), on-board outputs are reported as follows: A(1) = 253, B(2) = 254, C(3) = 255, and others report as 001 to 58. The output report is Relay Set Output #rrrr when the output is turned ON and Relay Set Output #rrrr when the output is turned off. Output reports are also stored in the control panel memory log.

Controlling Outputs

As mentioned, outputs can be activated depending upon events that exist with the control 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 CHG OUTPUTS? function to toggle outputs reserved for special functions. Special function outputs are Area and control panel Wide output functions as well as outputs assigned to KP# Entr Key Rly and Output Response 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 control panel and the Output C provides a path to common. Output C turns off the common connection during sensor reset..
Check output status after reprogramming or resetting the control panel. All outputs are turned off after the control panel is reset. Certain output functions are checked by the control 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:

Fire Bell	Area Fault	Part On Fault
Summary Fire	Summary Alarm	AC Fail
Summary Trouble	Phone Fail	Communications Fail
Silent Alarm	Watch Mode	Reset Sensors
Summary SupFire	Alarm Bell	Battery Trouble
Summary Fire Tbl	Area Armed	Summary SupBurg

These output functions need to be manually reset with Change Output function:

Fail To Close	Force Armed
Duress	Log % Full

8.1 Area Wide Outputs

Alarm Bell

Default: 1
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: A(1), B(2) or C(3), 0
This output activates when an intrusion point assigned to this area goes into alarm. It also activates for (non-fire) keypad and keyfob alarms that are configured to sound the Alarm Bell.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to a value other than **0** for each enabled area. Refer to SIA CP-01 Verification for more information.
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.
RPS Menu Location
Output Parameters > Area Wide Outputs > Alarm Bell

Fire Bell

Default: 1
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: 1(A), 2(B) or 3(C), 0
This output activates when a fire point assigned to this area goes into alarm. It will also activate for keypad fire alarms.
Fire Time and Fire Pattern 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. 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 meet UL 864 requirements, set this parameter to a value other than 0.
RPS Menu Location
Output Parameters > Area Wide Outputs > Fire Bell

Reset Sensors

Default: 3
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: 1(A), 2(B) or 3(C), 0
This parameter (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 event.
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.
RPS Menu Location
Output Parameters > Area Wide outputs > Reset Sensors

Fail To Close/Part On

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: 1(A), 2(B) or 3(C), 0

To change between the **Fail To Close** and **Part On** output functions described below, configure the Part On Output parameter.
for *Fail To Close* Operation
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 control 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

Force Armed

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: 1(A), 2(B) or 3(C), 0
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:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: A(1), B(2) or C(3), 0
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.
RPS Menu Location
Output Parameters > Area Wide Outputs > Watch Mode

Area Armed

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: A(1), B(2) or C(3), 0

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 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 control panel arming status.

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 > Area Armed

Area Off

Default: 0
Selections:
– **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– **B4512**: 1(A), 2(B) or 3(C), 0, 11-18, 21-28, 31-38
– **B3512**: 1(A), 2(B) or 3(C), 0

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 only activates 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 only de-activates 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 the 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 activates 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:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– B3512: A(1), B(2) or C(3), 0

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 a B308 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:

- B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- B4512: 1(A), 2(B) or 3(C), 0, 9-38
- B3512: 1(A), 2(B) or 3(C), 0

The output activates when a duress alarm is generated from a point 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.

RPS Menu Location

Output Parameters > Area Wide Outputs > Duress Output

Part On Fault

Default: 0

Selections:

- B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- B4512: 1(A), 2(B) or 3(C), 0, 9-38
- B3512: 1(A), 2(B) or 3(C), 0

The output activates when a controlled perimeter point (*Type 1*) 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 perimeter 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:

- B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- B4512: 1(A), 2(B) or 3(C), 0, 9-38
- B3512: A(1), B(2) or C(3), 0

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.

RPS Menu Location

Output Parameters > Area Wide Outputs > Silent Alarm

Gas Bell

Default: 1
Selections:
– **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– **B4512**: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
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 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

8.2 Panel Wide Outputs

AC Failure

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter enables the output to activate when the control panel responds to an AC power failure as programmed in AC Fail Time. The 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.
RPS Menu Location
Output Parameters > Panel Wide Outputs > AC Failure

Battery Trouble

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter enables the output to activate 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. The 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.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Battery Trouble

Phone Fail

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter enables the output to activate when a telephone line failure alarm is generated. The output automatically resets when a valid passcode is entered at the keypad.
A time must be entered in Phone Supervision Time in order for this output to activate.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Phone Fail

Comm Fail

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter enables the output to activate when the control panel is unable to send a report after 10 attempts are made to each routing destination. This output automatically resets when a report is sent successfully. Use this parameter to report primary digital report failure to an alternate communication device.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Comm Fail

Log % Full (Outputs)

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter sets the number of the output that activates when the log has reached the programmed percentage of its capacity as programmed in Log % Full. A steady output is provided until the RPS pointer is set.
RPS Menu Location
Output Parameters > control panel Wide Outputs > Log % Full (Outputs)

Additional resources
See Get History for more information.

Summary Fire

Default: 0
Selections:
– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0

This parameter sets the number of the output that activates when any fire point in the system (Point type = Fire) goes into alarm. A steady output is provided 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 (**> Misc > Fire Summary Sustain**) = **No**.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Fire

Summary Alarm

Default: 0

Selections:

– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0

This parameter sets 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.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Alarm

Summary Fire Trouble

Default: 0

Selections:

– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0

This parameter enables the output to activate when any fire point on the control panel is in trouble. A steady output is provided until all fire points have restored to a normal event and 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.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Fire Trouble

Summary Supervisory Fire

Default: 0

Selections:

– B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– B4512: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0

This output activates when any fire supervisory point on the control panel is in a supervisory event (off normal). A steady output is provided until all fire supervisory points are restored to a normal condition and 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.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Supervisory Fire

Summary Trouble

Default: 0

Selections:

- B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- B4512: 1(A), 2(B) or 3(C), 0, 9-38
- **B3512**: 1(A), 2(B) or 3(C), 0

This parameter output activates when any non-fire/gas point on the control panel is in a trouble condition. A steady output 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.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Trouble

Summary Supervisory Burg

Default: 0

Selections:

- B5512: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- B4512: 1(A), 2(B) or 3(C), 0, 9-38
- **B3512**: 1(A), 2(B) or 3(C), 0

This parameter enables the output to activate when any non-fire supervisory point on the control panel is in a supervisory condition. A steady output is provided until all Burg points are restored to a normal condition and 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.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Supervisory Burg

Summary Gas Output

Default: 0

Selections:

- **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
- **B4512**: 1(A), 2(B) or 3(C), 0, 9-38
- **B3512**: 1(A), 2(B) or 3(C), 0

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 and the event message is cleared by the user at the keypad.

RPS Menu Location

Output Parameters > Panel Wide Outputs > Summary Gas Output

Summary Gas Supervisory Output

Default: 0
Selections:
– **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– **B4512**: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
This parameter enables the output to activate when any gas supervisory point on the control panel is in a supervisory event (off normal). A steady output is provided until all gas supervisory points are restored to a normal condition and the event message is cleared by the user at the keypad.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Summary Gas Supervisory Output

Summary Gas Trouble Output

Default: 0
Selections:
– **B5512**: 1(A), 2(B) or 3(C), 0, 9-48, 50-58
– **B4512**: 1(A), 2(B) or 3(C), 0, 9-38
– **B3512**: 1(A), 2(B) or 3(C), 0
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 and the event message is cleared by the user at the keypad.
RPS Menu Location
Output Parameters > Panel Wide Outputs > Summary Gas Trouble Output

8.3 Output Configuration

Output Text

Default: Output #
Selections: Up to 32 alphanumeric characters
This parameter provides a description for the physical location of the point for use by installation and service personnel. Enter up to 32 characters of text to describe the output.
RPS Menu Location
Output Parameter > Output Configuration > Output Text

Output Source

Default:
– **B5512**:
– **Output A(1):** On-board
– **Output B(2):** On-board
– **Output C(3):** On-board
– **Outputs 9 to 58:** Unassigned
– **B4512**:
– **Output A(1):** On-board
– **Output B(2):** On-board
– **Output C(3):** On-board

– **Outputs 9 to 38:** Unassigned
– **B3512**:
– **Output A(1):** On-board
– **Output B(2):** On-board
– **Output C(3):** On-board

Selections:

On-Board	Output A, B and C are on-board outputs. This is a reference only selection.
Unassigned	The output is not assigned to an octo-output.
Octo-output	The output is installed on an SDI2 bus output module.
IP Camera	The output is installed on a camera. Can be used as a point source. See Point Source.

This parameter guides the RPS operator with configuration rules regarding where the Octo-output and IP Camera devices are allowed to be configured, and what output number ranges are permitted. You cannot change grayed out selections.
Optional installation and configuration:

- Install a B308 Octo-output module on particular Output number boundaries starting at Output 11. Refer to B308 Octo-output Switch Settings.
- Install an IP Camera on Output numbers 11-18, 21-28, 31-38, and 41-48.
- Use any of the selections as a point source. Refer to Point Source.

All Bosch IP cameras have integrated Video Content Analyses (VCA). VCA detects and analyzes changes in the picture using image processing algorithms. Changes in the picture can be due to movements in the camera's field of view. Detection of movement can be used to trigger an alarm and to transmit metadata.
Various VCA configurations can be selected and adapted to your application, as required.
These camera VCA conditions can generate output, or alarm conditions that can be used as the source for B Series control panel sensor inputs (example: Point Source). When an IP camera-to-control panel configuration is used, camera VCA alarm conditions will result in a faulted (shorted) point condition. B Series control panel functionality is unchanged, with the only exception being that an IP camera input device, or sensor is now allowed.

RPS Menu Location

Output Parameters > Output Configuration > Output Source

9 User Configuration

9.1 User Assignments

User Name

Default:
- User 0: Installer
- Users 1 to 50 (B5512 only): USER 1 - USER 50
- Users 1 to 32 (B4512 only): USER 1 - USER 32
- Users 1 to 10 (B3512 only): USER 1 - USER 10

Selections: 16 alphanumeric characters (enter using capital letters)
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).
Enter up to 16 characters of text for this user group.
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 (:).
User 0 applies only to passcodes and authority levels. There is no User 0 for access site codes and card data.
RPS Menu Location
User Configuration > User Assignments > User Name

Passcode

Default:
- **B5512**:
- User 0: 123
- User 1: 123456
- Users 2-50: Blank
- **B4512**:
- User 0: 123
- User 1: 1234(56)
- Users 2-32: Blank
- **B3512**:
- User 0: 123
- User 1: 1234(56)
- Users 2- 10: Blank

Selections: Enter a 3-to-6-digits based on the entry made in Passcode Length.
This parameter sets 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.
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.

RPS Menu Location

User Configuration > User Assignments (Passcodes) > Passcode

User Group

Default: 0

Selections:

- **B5512**: 0, 1, 2, 3, 4
- **B4512**: 0, 1, 2
- **B3512**: 0, 1, 2

This parameter creates a group of up to 50 users for the B5512, 32 users for the B4512, or 10 users for the B3512 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 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 0.
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.

RPS Menu Location

User Configuration > User Assignments (Passcodes) > User Group

Area# Auth

Default:

- User 0: 15
- **User 1:**
- B5512: A1 Authority = 1, A2 to A4 Authority = 0
- B4512: A1 Authority = 1, A2 Authority = 0
- B3512: A1 Authority = 1
- All Other User #'s: 0

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. Authority level 15 is reserved for User 0- Installer and cannot be changed.

RPS Menu Location

User Configuration > User Assignments > Area# Authority

User Language

Default: 1:(language programmed as first language in Panel Data window)
Selections: 1:(first language), 2:(second language)
This parameter sets the language to display at the assigned keypad.
First and Second languages are programmed during panel account setup in the New Panel Data window. Supported languages include English, Spanish, French and Portuguese.
RPS Menu Location
User Configuration > User Assignments (Passcodes) > User Language

9.2 Keyfob RFID/Card Data

User Name

Default: User #
Selections: 32 alphanumeric characters
This parameter sets what is displayed at keypads.
Enter up to 32 characters of text, numbers and symbols.
– 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.

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
User Configuration > Keyfob RFID/Card Data > User Name

Keyfob RFID (B820 Inovonics Wireless)

Default: N/A
Selections: 0 - 99999999
Each user can be assigned a wireless keyfob RFID (Radio Frequency device Identification number). An Inovonics 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 Inovonics keyfob replacement, or can be set to 0 to disable a user's Inovonics 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. Duplicate ID detection must be based on the RFID value stored in configuration memory, not on the number printed on the device. Inovonics keyfobs are not supervised when assigned to a user.
RPS Menu Location
User Configuration > Keyfob RFID/Card Data > Keyfob RFID (B820 Inovonics Wireless)

Keyfob RFID (B810 RADION Wireless)

Default: 0
Selections: 11 - 167772156
Each user can be assigned a wireless keyfob RFID (Radio Frequency device Identification number). A RADION 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 RADION keyfob replacement, or can be set to 0 to disable a user's RADION 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. Duplicate ID detection must be based on the RFID value stored in configuration memory, not on the number printed on the device.

RPS Menu Location

User Configuration > Keyfob RFID/Card Data > Keyfob RFID (B810 RADION Wireless)

Supervised

Default: No

Selections: Yes/No

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 supervises the presence of key fobs assigned to the area.

This parameter can be set individually for each key fob. When enabled, the keyfob is supervised in four-hour intervals.

Note: Keyfobs are not supervised when assigned to a user.

RPS Menu Location

User Configuration > Keyfob RFID/Card Data > Supervised

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.

RPS Menu Location

User Configuration > Keyfob RFID/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).
RPS Menu Location
User Configuration > Keyfob RFID/Card Data > Card Data

9.3 User (Keypad) Functions

All On Delay

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function arms all Delay areas that are disarmed.
When the passcode is entered at the keypad, the control panel checks the user's authority level.
RPS Menu Location
User Configuration > User Keypad Functions > All On Delay

All On Instant

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function arms all Instant areas that are disarmed.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Disabled (-)**. Refer to SIA CP-01 Verification for more information.
Entry and Exit Delays **are not** provided with this arming function. This causes Part On and interior delay points to act as instant points.
RPS Menu Location
User Configuration > User Keypad Functions > All On Instant

Part On Instant

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function turns areas part on with no entry/exit delays in the area where the keypad is assigned. This causes perimeter and interior delay points to act as instant points.
IMPORTANT: To comply with SIA CP-01 False Alarm Reduction, set this parameter to **Disabled (-)**. Refer to SIA CP-01 Verification for more information.
RPS Menu Location
User Configuration > User Keypad Functions > Part On Instant

Part On Delay

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function turns areas part on with entry/exit delays 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.
RPS Menu Location
User Configuration > User Keypad Functions > Part On Delay

Watch Mode

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function turns watch mode on and off.
This function provides keypad audible/visual and optional output activation when a point configured for Watch Mode is activated. (Refer to Watch Mode in the Area Wide Outputs section).
RPS Menu Location
User Configuration > User Keypad Functions > Watch Mode

View Area Status

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to view the armed status of all areas within the scope of the keypad.
The armed states include:
- Disarmed
- All On delay armed
- All On instant armed
- Part On instant armed
- Part On delay armed

All area types (Master, Associate, Regular and Shared) can be viewed using this function.
RPS Menu Location
User Configuration > User Keypad Functions > View Area Status

View/Delete Event Memory

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to view and delete event memory. Event memory is not deleted until the area is rearmed.
RPS Menu Location
User Configuration > User Keypad Functions > View/Delete Event Memory

View Point Status

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to view point status, point text and the electrical state (normal, open, short and missing) of each point assigned to the area.
RPS Menu Location
User Configuration > User Keypad Functions > View Point Status

Walk Test (All Non-Fire Burg Points)

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
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.
RPS Menu Location
User Configuration > User Keypad Functions > Walk Test (All Non-Fire Burg Points)

Walk Test All Fire Points

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
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, Point Type, cannot be tested using the fire walk test mode. 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.
RPS Menu Location
User Configuration > User Keypad Functions > Walk Test All Fire Points

Send Report (Test/Status)

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function tests the communication link between the control panel and the central station receiver(s).
This parameter 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.
RPS Menu Location
User Configuration > User Keypad Functions > Send Report (Test/Status)

Set Keypad Brightness/Volume/Keypress

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to select either a bright or dim display with loud or soft keypad warning tones.
RPS Menu Location
User Configuration > User Keypad Functions > Set Keypad Brightness/Volume/Keypress

Set/Show Date and Time

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to set the time and date in the control panel.
RPS Menu Location
User Configuration > User Keypad Functions > Set/Show Date and Time

Change Passcode

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows a user to change their own passcode.
This is a panel wide function that can be executed from any keypad assigned to an area where the user has authority. Regardless of whether an E or a P is placed here, the keypad will prompt the user to enter their existing passcode first.
RPS Menu Location

User Configuration > User Keypad Functions > Change Passcode

Add/Edit User

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows a user with authority to add or change passcodes, and add or change control panel authority levels for other users by area.
RPS Menu Location
User Configuration > User Keypad Functions > Add/Edit User

Delete User

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows a user with authority to delete other users' passcodes. It does not delete user names.
RPS Menu Location
User Configuration > User Keypad Functions > Delete User

Extend Close

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows users to extend the closing window.
The window cannot be adjusted until the Close Early Begin time has passed and the closing window is active.
RPS Menu Location
User Configuration > User Keypad Functions > Extend Close

View Event Log

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to view the event log.
RPS Menu Location
User Configuration > User Keypad Functions > View Event Log

Bypass a Point

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function bypasses individual points in areas within the Scope of the keypad. Bypassed points do not create alarm or trouble events.
RPS Menu Location
User Configuration > User Keypad Functions > Bypass a Point

Unbypass a Point

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function unbypasses individual points that are programmed either P## FA Returnable or P## Bypass Returnable. Points within the Scope of the keypad are unbypassed where the function is entered.
The control panel will respond to alarms/troubles and display point faults when a point is unbypassed.
RPS Menu Location
User Configuration > User Keypad Functions > Unbypass a Point

Reset Sensors

Default: E
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function resest sensors in areas within the Scope of the keypad.
RPS Menu Location
User Configuration > User Keypad Functions > Reset Sensors

Change Outputs

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to manually set and reset any outputs installed in the system.

NOTE: The Change Outputs parameter also works with onboard outputs. Use the following output numbers to toggle the onboard outputs:

– Onboard Output A(1) > Output #253
– Onboard Output B(2) > Output #254
– Onboard Output C(3) > Output #255

RPS Menu Location

User Configuration > User Keypad Functions > Change Outputs

Remote Program

Default: P

Selections: - , E, P

Disable (-) Disable this function panel wide regardless of the user's authority level.

Enable (E) Enable this function panel wide without requiring a passcode.

Passcode (P) Require a passcode to enable this function panel wide.

This function initiates Remote Account Manager sessions. When the phone is ringing at the control panel, the user initiates this function to have the control panel seize the line.

RPS Menu Location

User Configuration > User Keypad Functions > Remote Program

Go to Area

Default: P

Selections: - , E, P

Disable (-) Disable this function panel wide regardless of the user's authority level.

Enable (E) Enable this function panel wide without requiring a passcode.

Passcode (P) Require a passcode to enable this function panel wide.

This function temporarily switches 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.

RPS Menu Location

User Configuration > User Keypad Functions > Move to Area

Display Panel Type and Revision

Default: E

Selections: - , E, P

Disable (-) Disable this function panel wide regardless of the user's authority level.

Enable (E) Enable this function panel wide without requiring a passcode.

Passcode (P) Require a passcode to enable this function panel wide.

This function displays the control panel's software revision number in the keypad display.

RPS Menu Location

User Configuration > User Keypad Functions > Display Revision

Service Walk All Points

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows a user to walk test all points in the entire control panel regardless of the Point Type.
24-Hour points left off-normal when exiting the Service Walk Test are bypassed. A trouble tone sounds until it is silenced. The keypads alternate text with the Bypass indications.
RPS Menu Location
User Configuration > User Keypad Functions > Service Walk All Points

Change Skeds

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows the user to change the Time from the keypad to make adjustments to Skeds. This is a panel wide function that can be executed from any keypad assigned to an area where the user has authority.
RPS Menu Location
User Configuration > User Keypad Functions > Change Skeds

Walk Test All Invisible Burg Points

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows a user with Invisible Walk Test authority to test invisible intrusion 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.
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.
RPS Menu Location
User Configuration > User Keypad Functions > Walk Test All Invisible Burg Points

Custom Functions 128 to 131

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function sets 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. The B5512 supports Custom Function 128, 129, 130 and 131. The B4512 supports Custom Function 128 and 129. The B3512 supports Custom Function 128.
RPS Menu Location
User Configuration > User Keypad Functions > Custom Functions 128 to 131

Keypad Programming

Default: P
Selections: - , E, P
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
Passcode (P) Require a passcode to enable this function panel wide.
This function allows local keypad programming for a select list of parameters from keypads.
The Installer 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.
RPS Menu Location
User Configuration > User Keypad Functions > Keypad Programming
Additional resources
Refer to the control panel documentation for more information on keypad programming.

9.4 Authority Levels

Authority Levels Overview

Authority Levels - Level # -->	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disarm Select	E	E	E	E	E	-	-	-	-	-	-	-	-	E	-
All On Delay	E	E	E	E	E	-	-	-	-	-	-	-	-	-	-
All On Instant	E	E	-	-	-	-	-	-	-	-	-	-	-	-	-
Part On Instant	E	E	E	E	-	-	-	-	-	-	-	-	-	-	-
Part On Delay	E	E	E	E	-	-	-	-	-	-	-	-	-	-	-
Watch Mode	E	E	E	-	-	-	-	-	-	-	-	-	-	-	E
View Area Status	E	E	-	-	-	-	-	-	-	-	-	-	-	-	E
View Event Memory	E	E	E	-	-	-	-	-	-	-	-	-	-	-	E
View Point Status	E	E	E	-	-	-	-	-	-	-	-	-	-	-	E
Walk Test (All Non-Fire Burg Points)	E	E	-	-	-	-	-	-	-	-	-	-	-	-	E
Walk Test All Fire Points	E	E	-	-	-	-	-	-	-	-	-	-	-	-	E
Send Report (Test/Status)	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Change Keypad Display	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Change Date and Time	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Change Passcodes	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Add User Passcode/Card/Level	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Delete User Passcode/Card/Level	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Extend Close	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
View Event Log	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Bypass a Point	E	E	E	E	-	-	-	-	-	-	-	-	-	-	E
Unbypass a Point	E	E	E	E	-	-	-	-	-	-	-	-	-	-	E
Reset Sensor(s)	E	E	E	E	-	-	-	-	-	-	-	-	-	-	E
Change Output(s)	E	E	-	-	-	-	-	-	-	-	-	-	-	-	E
Remote Program	E	E	E	E	-	-	-	-	-	-	-	-	-	-	E
Go to Area	E	E	-	-	-	-	-	-	-	-	-	-	-	-	E
Display Panel Type and Revision	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Service Walk All Points	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Change Skeds	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Walk Test All Invisible Burg Points	E	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Custom Function 128	E	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Custom Function 129	E	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Custom Function 130	E	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Custom Function 131	E	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Force Arm	E	E	E	E	E	E	-	-	-	-	-	-	-	-	-
Send Area Opening/Closings	E	E	E	E	E	E	E	E	E	E	E	E	E	E	-
Restricted Open/Close	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Part On Open/Close	E	E	E	E	E	E	E	E	E	E	E	E	E	E	-
Send Duress	-	-	-	-	-	-	-	-	-	-	-	-	-	E	-
Arm By Passcode	E	E	E	E	E	E	-	-	-	-	-	-	-	-	-
Disarm By Passcode	E	E	E	E	E	-	-	-	-	-	-	-	-	E	-
Keyfob Arm/Disarm	E	E	E	E	E	E	-	-	-	-	-	-	-	-	-
Firmware Update	E	E	E	E	E	E	-	-	-	-	-	-	-	-	-

Refer to the following topics for detailed information:

[Disarm Select]
[All On Delay]
[All on Instant]
[Part On Instant]
[Part On Delay]
[Watch Mode]
[View Area Status]
[View Event Memory]
[View Point Status]
[Walk Test (all non-fire burg points)]
[Walk Test (fire points)]
[Walk Test all invisible burg points]
[Service Walk All Points]
[Send Report (test/status)]
[Change Keypad Display]
[Change Date/Time]
[Change Passcode]
[Add User (passcode/card/level)]
[Delete User (passcode/card/level)]
[Extend Close]

View Event Log
Bypass a Point
Unbypass a Point
Reset Sensors
Change Outputs
Remote Program
Go to Area
Display Panel Type/Revision
Change Skeds
Custom Function 128 to 131
Force Arm
Send Area Opening/Closings
Restricted Open/Close
Part On Open/Close
Send Duress
Arm by Passcode
Disarm by Passcode
Keyfob Arm
Keyfob Disarm
Firmware Update

Disarm Select

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

Selections:

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 parameter disarms 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.
The options available for arming and disarming are dependent upon Area Type and Scope.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
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 that the following parameters are enabled:

– Disarm
– Send Duress
– Passcode Disarm

RPS Menu Location

User Configuration > Authority Levels > Disarm Select

Additional resources

Area Type
Scope
Duress Type
Send Duress
Passcode Disarm

All On Delay

Default:

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > All On Delay

All On Instant

Default:

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

Selections:

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.

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 entering MENU 112, the area scope is restricted to the current area of the keypad.

RPS Menu Location
User Configuration > Authority Levels > All On Instant

Part On Instant

Default:
– Authority Levels **1-4:** Enabled (E)
– Authority Levels **5-15:** Blank (-)
Selections:
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.
This parameter allows a user to arm all perimeter points in areas that correspond to the user's Authority Level with no exit delay time.
When Part On Delay is accessed by entering MENU 121, the area scope is restricted to the current area of the keypad.
Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
RPS Menu Location
User Configuration > Authority Levels > Part On Instant

Part On Delay

Default:
– Authority Levels **1-4:** Enabled (E)
– Authority Levels **5-15:** Blank (-)
Selections:
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.
This parameter allows a user to arm all perimeter points in areas that correspond to the user's Authority Level with exit delay.
Authority Level 15 is reserved for the Service Passcode (User 0). You cannot change any settings in the Authority Level 15 column.
RPS Menu Location
User Configuration > Authority Levels > Part On Delay

Watch Mode

Default:
– Authority Levels **1-3, 15:** Enabled (E)
– Authority Levels **4-14:** Blank (-)
Selections:
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.
This parameter allows the user with this authority level to initiate the watch mode in the area to which this is keypad assigned.

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

RPS Menu Location

User Configuration > Authority Levels > Watch Mode

View Area Status

Default:

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > View Area Status

View Event Memory

Default:

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > View Event Memory

View Point Status

Default:

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

Selections:

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.

This parameter allows the user with this authority level to view the current status of all points in the area to which this keypad is assigned.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
RPS Menu Location
User Configuration > 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:
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a 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.
RPS Menu Location
User Configuration > Authority Levels > Walk Test (non-fire burg points)

Walk Test All Fire Points

Default:
– Authority Levels **1, 2, 15:** Enabled (E)
– Authority Levels **3-14:** Blank (-)
Selections:
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.
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 Walk Test All Fire Points 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 control 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 control 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 Resettable as YES.
– The keypad displays a sequential count after each point is activated and restored as well as the text for the point.
– `FIRE WALK START and FIRE WALK END` are reported at the central station receiver for the beginning and end of the test.
Fire 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.
RPS Menu Location
User Configuration > Authority Levels > Walk Test All Fire Points

Walk Test All Invisible Burg Point

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

Selections:
Disable (-) Disable this function panel wide regardless of the user's authority level.
Enable (E) Enable this function panel wide without requiring a passcode.
This function 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.
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.
RPS Menu Location
User Configuration > Authority Levels > Walk Test All Invisible Burg Point
Additional Information
Authority Levels Overview

Service Walk All Points

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

Selections:
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.
This parameter allows the user with this authority level to initiate a service walk test for all 24 hour interior and perimeter controlled points in the control 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 or Part On.
When a Service Walk Test is initiated, one person can test all the points in the control panel without assistance.
Points 128 and Point 248 are not accessible by this function. This is normal. 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.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

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.

RPS Menu Location

User Configuration > Authority Levels > Service Walk All Points

Send Report (Test/Status)

Default:

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Send Report (Test/Report)

Change Keypad Display

Default:

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

Selections:

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.

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

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > 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)

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.

This parameter allows the user with this authority level to change and display the date and time for the control panel in this area.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
RPS Menu Location
User Configuration > Authority Levels > Change Date and Time

Change Passcode

Default:
– Authority Levels **1, 15:** Enabled (E)
– Authority Levels **2-14:** Blank (-)
Selections:
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.
This parameter allows the user with this authority level to change a user passcode.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
RPS Menu Location
User Configuration > Authority Levels > Change Passcode

Add User passcode/card/level

Default:
– Authority Levels **1, 15:** Enabled (E)
– Authority Levels **2-14:** Blank (-)
Selections:
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.
This parameter allows the user with this authority level to add/change users.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
RPS Menu Location
User Configuration > 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 (-) 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.
This parameter allows the user with this L## to delete users.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Delete User passcode/card/level

Extend Close

Default: Service Walk

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

Selections:

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.

This parameter allows the user with this authority level to change the closing time in the area where the function is entered.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Extend Close

View Event Log

Default:

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

Selections:

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.

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

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > View Event Log

Bypass a Point

Default:

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

Selections:

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

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Bypass a Point

Unbypass a Point

Default:

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

Selections:

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.

This parameter allows the user with this authority level to unbypass points. Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Unbypass a Point

Reset Sensors

Default:

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

Selections:

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.

This parameter allows the user with this authority level to reset sensors. Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Reset Sensors

Change Outputs

Default:

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

Selections:

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.

This parameter allows the user with this authority level to set OUTPUT ON and reset OUTPUT OFF outputs in the control panel.

Do not 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 Enter Key Output.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Change Outputs

Remote Program

Default:

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

Selections:

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.

This parameter allows the user with this authority level to initiate an RPS session when the phone rings at the control panel.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Remote Programming

Go to Area

Default:

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

Selections:

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.

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.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Go to Area

Display Panel Type and Revision

Default:

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

Selections:

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.

This parameter allows the user with this authority level to display the control panel firmware revision. All keypads will display the firmware revision as a Major.Minor.Micro value with the following format ##.##.###.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Display Panel Type and Revision

Change Skeds

Default:

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Change Skeds

Custom Functions 128 to 131

Default:

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

Selections:

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.

Allow the user with this authority level to execute the desired Custom Function.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

The B5512 supports Custom Function 128, 129, 130 and 131. The B4512 supports Custom Function 128 and 129. The B3512 supports Custom Function 128.

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.

RPS Menu Location

User Configuration > Authority Levels > Custom Functions 128 to 131

Force Arm

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

Selections:

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.

Allow a user with this authority level to force arm the control panel.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Force Arm

Send Area Opening/Closings

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

Selections:

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.

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.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Send Area Opening/Closings

Restricted Open/Close

Default: Blank (-) for all authority levels

Selections:

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.

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 (Refer to Restricted O/C).
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Restricted Open/Close

Part On Open/Close

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

Selections:

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.

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.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Part On Open/Close

Send Duress

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

Selections:

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.

Allow a user with this authority level to send duress report if the area to which this authority level is assigned sends duress. Refer to Duress Enable for more information.

Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

Configure the Duress Enable parameter to **Yes** in applicable areas, or the keypad will respond with *No Authority*.

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 the following functions to be enabled:
- Disarm
- Send Duress
- Passcode Disarm

RPS Menu Location

User Configuration > Authority Levels > Send Duress

Duress Enable
Duress Type
Disarm
Passcode Disarm

Arm by Passcode

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

Selections:

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.

Allow a user with this authority level to arm an area by entering their passcode, then pressing the [ENTER] key.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location
User Configuration > Authority Levels > Arm by Passcode

Disarm by Passcode

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

Selections:

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.

Allow a user with this authority level to disarm an area by entering their passcode, then pressing the [ENTER] key.
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.
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 the following functions to be enabled:
- Disarm
- Send Duress
- Disarm by Passcode

RPS Menu Location
User Configuration > Authority Levels > Disarm by Passcode

Additional resources
Duress Enable
Duress Type
Disarm

Send Duress

Keyfob Arm

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

Selections:

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.

Allow a user with this authority level to arm an area using their assigned keyfob. Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

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.

RPS Menu Location

User Configuration > Authority Levels > Keyfob Arm

Keyfob Disarm

Default: Blank (-)

Selections:

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.

Allow a user with this authority level to disarm an area by using their assigned keyfob. Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

Duress operation when disarming is not applicable when using key fobs.

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.

RPS Menu Location

User Configuration > Authority Levels > Keyfob Disarm

Firmware Update

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

Selections:

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.

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).
Authority Level 15 is reserved for the Service Passcode (User 0) and cannot be changed.

RPS Menu Location

User Configuration > Authority Levels > Firmware Update

10 Points

10.1 Point Assignments

Point Source

Default:
– **Points 1-8** On-board
– **All Other Points** Unassigned

Selections:

Unassigned	Point is not in use.
Output	Logical connection to the output of the same number. Not assigned to a physical device.
Octo-input	Point is assigned to an SDI2 bus input module.
Wireless	Point is assigned to an SDI2 bus RF receiver.
On-board	Point is assigned to the control panel.
Keypad	Point is assigned to a keypad.
IP Camera	Logical connection to a camera.

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.
Note: Point Source for points 1-8 is fixed as on-board and cannot be changed.
All Bosch IP cameras have integrated Video Content Analyses (VCA). VCA detects and analyzes changes in the picture using image processing algorithms. Changes in the picture can be due to movements in the camera's field of view. Detection of movement can be used to trigger an alarm and to transmit metadata.
Various VCA configurations can be selected and adapted to your application, as required.
These camera VCA conditions can generate output, or alarm conditions that can be used as the source for B Series control panel sensor inputs (example: Point Source). When an IP camera-to-control panel configuration is used, camera VCA alarm conditions will result in a faulted (shorted) point condition. B Series control panel functionality is unchanged, with the only difference being that an IP camera input device (used as a sensor) is now allowed.
RPS Menu Location
Points > Point Assignments > Source

Text

Default: Point #
Selections: Up to 32 characters.
This parameter sets what is displayed at keypads and what is reported to the central station receiver when transmitting in Modem4 format (if it is a reporting point).
Enter up to 32 characters of text, numbers and symbols to describe the point.
– 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.

Note: Include the point number in custom point text. This helps the user when viewing events, initiating bypasses, etc. and can simplify troubleshooting.

RPS Menu Location

Points > Point Assignments > Text

Point Text- second language

Default: Blank

Selections: Up to 32 characters.

This parameter sets what is displayed at keypads and what is reported to the central station receiver when transmitting in Modem4 format (if it is a reporting point). Enter up to 32 characters from the Latin-1 8-bit (ISO/IEC 8859-1) character set to describe the area.

– 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.

Note: Include the point number in custom point text. This helps the user when viewing events, initiating bypasses, etc. and can simplify troubleshooting.

RPS Menu Location

Points > Point Assignments > Second Language

Point Index (point profile)

Default:

– Point 1: 4
– Point 2: 8
– Point 3: 8
– Point 4: 13
– Point 5: 13
– Point 6: 7
– Point 7: 7
– Point 8: 1
– Points 9 to 48: 0

Selections: 0 to 20

This parameter selects one of the 20 point index (point profiles) that define the points' characteristics and determine how the control panel responds to various point events.

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).

RPS Menu Location

Points > Point Assignments > Index

Index (point profile) Description

Default: Points 1-8: blank, All other points Unassigned
Selections: No selections – this field cannot be edited by the user
This field displays a description of the point index (point profile) that is entered in the Index Description field. It is a reference field only and the information displayed in it is not sent to the control panel.
RPS Menu Location
Points > Point Assignments > Description

Area

Default: 1
Selections:
- B5512: 1 to 4
- B4512: 1 to 2
- B3512: 1

The areas are numbered 1 to 4. Select the area number you want the point assigned to.
- The B5512 supports Points 1 to 48. The B4512 supports Points 1 to 28. The B3512 supports Points 1 to 16.
- The B5512 supports up to 4 areas. The B4512 supports up to 2 areas. The B3512 supports 1 area.

RPS Menu Location
Points > Point Assignments > Area

Debounce

Default: 500 ms
Selections:

Scans	Debounce	Scans	Debounce	Scans	Debounce	Scans	Debounce	Scans	Debounce
1	250 ms	6	1.50 s	11	2.75 s	16	4.00 s	21	5.25 s
2	500 ms	7	1.75 s	12	3.00 s	17	4.25 s	22	5.50 s
3	750 ms	8	2.00 s	13	3.25 s	18	4.50 s	23	5.75 s
4	1s	9	2.25 s	14	3.50 s	19	4.75 s	24	6.00 s
5	1.25 s	10	2.50 s	15	3.75 s	20	5.00 s		

This parameter sets the number of times the control panel scans a point before initiating an alarm. Scan cycles are 250 ms. For appropriate settings, consult the manufacturer's instructions for the device connected to this point.
Bosch recommends an entry of 500 ms or higher. Interior follower points should have a debounce of at least 750 ms.

Debounce does not apply when the Point Source is set to Wireless or Output. 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:

B5512**:** 0, A(1), B(2), C(3), 9-58

B4512: 0, 1-3, 9-38

B3512: 0, 1-3

Use this parameter to activate an output when the point goes into alarm.

The output does not activate for Trouble or Supervisory events. Reset the output by clearing the memory from the keypad display.

RPS Menu Location

Points > Point Assignments > Output

RADION RFID (B810)

Default: - blank

Selections: 0 - 167772156

A point Radio Frequency device Identification number (RFID) can be Auto-Learned through the SDI2 bus RF receiver, or it can be entered here.

Auto-Learned RFID's can be edited for point replacement, or can be set to 0 to disable a RF point. 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.

If an SDI2 communication device is allocated for automation communication, then it cannot be used for central station or RPS communication.

When the Point Source is configured to Wireless, then the RFID is set to 0.

RPS Menu Location

Points > Point Assignments > RADION RFID (B810)

RADION Device Type

Default:

- If no wireless device is selected: (-)
- If a wireless device is selected: Door Window Contact

Selections:

- Glass Break
- Smoke
- Inertia
- Door Window Contact
- Recessed Door Window
- Motion Dual
- Motion PIR
- Ceiling Mt.Motion
- Universal TX
- Bill Trap

– Curtain Motion
– CO Detector
– Panic, One Button
– 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
Glass Break	Glass Break Alarm	Not Used	Not Used	Not Used
Smoke	Smoke Alarm	Not Used	Not Used	Not Used
Inertia	Reed Alarm	Loop Input	Vibration Alarm	Not Used
Door Window Contact	Reed Alarm	Not Used	Not Used	Not Used
Recessed Door Window	Reed Alarm	Not Used	Not Used	Not Used
Motion Dual	Motion Alarm	Not Used	Not Used	Not Used
Motion PIR	PIR Alarm	Not Used	Not Used	Not Used
Ceiling Mount Motion	Motion Alarm	Not Used	Not Used	Not Used
Universal TX	Reed Alarm	Loop Input	Not Used	Not Used
Bill Trap	Bill Trap Alarm	Not Used	Not Used	Not Used
Curtain Motion	PIR Alarm	Not Used	Not Used	Not Used
CO Detector	CO Alarm	Not Used	Not Used	Not Used
Panic, One Button	Not Used	Not Used	Not Used	Not Used
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 Device Type

Inovonics RFID (B820)

Default: N/A
Selections: 0 - 167772156
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. An 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.
If the configuration option, **Wireless Module Type**, is set to B820 Inovonics Wireless, the control panel is limited to 350 wireless devices not including repeaters.
Wireless is only a valid option if the number of points with **Point Source** set to Wireless plus the number of users assigned a valid key fob RF ID is less than 350.
Both the control panel and RPS enforce this restriction. Note, **Point Source** is used instead of RF ID as the installer might have assigned several points to wireless without adding any RF IDs.
When the Point Source is configured to Wireless then the RFID will be set to 0.
If an SDI2 communication device is allocated for automation communication, then it cannot be used for central station nor for RPS communication.
RPS Menu Location
Points > Point Assignments > RFID (B820 Inovonics Wireless)

10.2 Cross Point Parameters

Cross Point Timer

Default: 20
Selections: 5-255 (seconds)
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.
Only use the Cross Point function on non-fire points.
IMPORTANT Cross points must be overlapped so that each individual cross point can protect the area individually.
RPS Menu Location
Points > Cross Point Parameters > Cross Point Timer

10.3 Point Indexes (point profiles)

Point Index (point profiles) Overview

Use the point indexes to construct point profiles for points used in the system. The Index numbers are used in Point Assignments. Each unique point index number determines the control panel's responses to specific conditions occurring on the points.

Index Descriptions

Default:

– Point Index 1: 24-hr Instant Open/Short

An open or short condition on points assigned to this default index create an alarm instantly whether the system is on (armed) or off (disarmed). Use this default point index for points connected to emergency buttons.

– Point Index 2: 24-hr Inv/Sil on Short (Invisible/Silent on Short)

Alarms for points assigned to this Index do not activate sirens, bells, or the keypad sounder. They are not visible at the keypad. Typically used for points connected to hold-up buttons.

– Point Index 3: Pull Station

An open condition creates a trouble event. A short condition creates a fire alarm event. Use this default point index for points connected to Fire Pull Stations.

– Point Index 4: Smoke Detector

An open condition creates a trouble event. A short condition creates a fire alarm event. Reset function is enabled. Use this default Point Index for points connected to smoke detectors.

– Point Index 5: Smoke Det w/Verification (Smoke Detector with Verification)

An open condition creates a trouble event. A short condition creates a fire alarm event. Alarm verification function is enabled. Use this default Point Index for points connected to smoke detectors and where you want to use the panel's alarm verification feature.

– Point Index 6: Bell Supervision - D192G

Use this default point index for points connected to the D192G Notification Appliance Circuit Module (bell supervision module) SUPV ZONE terminal.

– Point Index 7: Part On: Instant

An open or short condition creates a instant alarm event when All On or Part On. Use this default point index for points connected to perimeter points (doors or windows) that are *not* used during exit or entry delay.

– Point Index 8: Part On: Delay

An open condition creates a instant alarm event when All On or Part On. An open or short condition starts entry delay when All On or Part On. Use this default point index for points connected to perimeter points (doors or windows) that are used during exit or entry delay.

– Point Index 9: Prt: Inst Local:Dis (Part On, Instant, Local While Arm

An open or short condition creates a instant alarm event when All On or Part On. An open or short condition creates a local alarm event when Off (disarmed). Use this default point index for points connected to perimeter points (doors or windows) that are *not* used during exit or entry delay.

– Point Index 10: Interior: Instant

An open or short condition creates a instant alarm event when All On. Use this default point index for points connected to interior points (motion detectors or interior doors) that are *not* faulted during exit or entry delay.

– **Point Index 11: Interior: Delay**

An or short condition starts entry delay when All On. Use this default point index for points connected to interior points (motion detectors or interior doors) that are used to start entry delay.

– **Point Index 12: Int: Inst Local:Dis** (Interior, Instant, Local While Disarmed)

An open or short condition creates a instant alarm event when All On. An open or short condition creates a local alarm event when Off (disarmed). Use this default point index for points connected to interior points (motion detectors or interior doors) that are *not* faulted during exit or entry delay.

– **Point Index 13: Interior: Follower**

Follows entry and exit delay. No alarm event during entry and exit delay. An open or short condition creates an alarm event when All On. Use this default point index for points connected to interior points (motion detectors or interior doors) that are faulted during exit or entry delay.

– **Point Index 14: Maintained Keyswitch**

Use this default Point Index for points connected to maintained keyswitches. Normal to short condition turns On (arms). Short condition to normal turns Off (disarms). Open condition is trouble when Off (disarmed), alarm when On (armed).

– **Point Index 15: Momentary Keyswitch**

Use this default Point Index for points connected to momentary keyswitches. Normal to short to normal condition toggles On (armed) and Off (disarmed). Open condition is trouble when Off (disarmed), alarm when On (armed).

– **Point Index 16: Open/Close on Fault**

Use this default Point Index for individual point arming and disarming. Short to normal arms the point and sends point closing report. Normal to Short disarms the point and sends point opening report. Open condition while armed is alarm, while disarmed is trouble.

– **Point Index 17: Gas**

Use this default Point Index for points connected to gas detectors (carbon monoxide detectors for example). Short condition on point creates gas alarm event.

– **Point Index 18: Gas: Supervisory**

Use this default Point Index for points connected to gas detectors (carbon monoxide detectors for example). Short condition on point creates gas supervisory event.

– **Point Index 19: Aux AC Supervision**

Use this default Point Index for points connected to the AC power fail outputs (relays) of auxiliary power supplies.

– **Point Index 20: Part On: Watch Off**

Use this default Point Index for perimeter points where the Watch function is not required.

Selections: Up to 24 alphanumeric characters

Enter up to 24 characters of text to describe the point index (point profile).

This is for informational purposes only and is not programmed in the control panel.

RPS Menu Location

Points > Point Indexes > Index Description

Point Type

Default:
- Point Indexes 1 to 2, 6: 24 Hour
- Point Indexes 3 to 5: Fire Point
- Point Indexes 7-9, 20: Part On
- Point Index 10 to 12: Interior
- Point Index 13: 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: (Reference Index Descriptions below)
This parameter defines the point type.
Index Descriptions:

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 perimeter point type with a Point Response of 9 to E. 24-hour points do not show faults when an arming function is entered, but perimeter points do. When programming for this type of protection, you should consider using the Buzz On Fault and Local While Disarmed options.
Hold-up devices in UL installations: the 24-Hour point type must be used for points connected to hold-up devices. The point text must include, “hold-up”.

Part On
Perimeter points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using part on 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.
Perimeter points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.
When a Perimeter Point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Perimeter Point trips, the control panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Perimeter Point's entry delay time is less than the remaining time, it shortens the entry delay time.
Perimeter 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 all on the area. They are not armed when using part on 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 (Refer to 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 (Refer to 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 the area. They are not armed when using part on 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 devices.

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 an instant alarm response is activated (Refer to 24-hour point response section). Fire alarms are the highest priority event in the control panel.

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 event 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 a Gas Alarm when an 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.

RPS Menu Location

Points > Point Indexes 1-20 > 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 perimeter point with a point Response of D and E displays at the keypad when arming. Like a 24-hour point, a point programmed this way can generate alarms whether the area is armed or disarmed.
Combining Point Response 9 with the Local While Disarmed feature provides off-site reporting when the area is armed, but only local alarm annunciation when the area is disarmed.
Combining Point Response 9 with the Local While Armed feature provides off-site reporting when the area is disarmed, but only local alarm annunciation when the area is armed.
Point Response E Use this for Asic motion detectors. This allows troubles to report while the control panel is all on.
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
1 Reporting: Fire reports are the first events that the control panel sends when a group of events occur.
2 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.
3 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.
4 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.
5 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.
6 Reset Sensor: A fire device that requires resetting can be manually reset using the reset sensor output for the area it is assigned to.
7 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.

Point Response

Default: (Reference the tables below for a description of the response value)
– Point Index 1, 7, 19, 20: 0
– Point Indexes 2-5, 14-17: 1
– Point Index 6, 18: 9
– Point Index 8, 11, 13: 8
– Point Index 9, 12: 9
– Point Index 10: 0
Selections: 0 - 9, A - F
This parameter 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. Perimeter 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 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 event as an open. As a result, typical Point Responses for the 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.

RPS Menu Location

Points > Point Indexes 1-20 > Point Response

Entry Delay

Default: 30 seconds

Selections: 5 - 600 seconds (5-second increments)

This parameter sets 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.

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. Refer to SIA CP-01 Verification for more information.

On the keypad's display, DISARM NOW appears for the duration of the time programmed when the point is faulted in the delay event. 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 perimeter 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.
RPS Menu Location
Points > Point Indexes 1-20 > Entry Delay

Entry Tone Off

Default: No (for all Point Indexes)
Selections: Yes/No
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.
This parameter enables/disables the entry delay warning tone for this point.
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.
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.
RPS Menu Location
Points > Point Indexes 1-20 > Entry Tone Off

Silent Bell

Default:
– Point Index 1, 3-20: No
– Point Index 2: Yes
Selections: Yes/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 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.

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.

RPS Menu Location
Points > Point Indexes 1-20 > Silent Bell

Ring Until Restored

Default: No (for all Point Indexes)
Selections: Yes/No

Yes Fire or Gas Bell output and keypad sounders for this point cannot be deactivated, from a keypad or upon bell time-out, until the point is restored to normal.

No Fire or Gas Bell output and keypad alarm sounders for this point can be deactivated, either from a keypad or upon bell time-out, whether or not the point has been restored to normal.

Use this parameter for fire or gas applications to meet the requirement that audible alarms cannot be silenced until the fault event clears.
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.

RPS Menu Location
Points > Point Indexes 1-20 > 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.

RPS Menu Location
Points > Point Indexes 1-20 > Audible After 2 Fails

Invisible Point

Default:
- Point Index 1: No
- Point Index 2: Yes

– Point Indexes 3 to 20: No

Selections: Yes/No

Yes Keypads do not display alarm activity from this point.

No Activity from this point is visible at the keypads.

This parameter determines whether the point appears in the keypad display upon an alarm event. Point text appears and annunciation is made for invisible points that are programmed for a trouble event in point response.

To prevent the keypad alarm tone and the Alarm Bell from sounding, this point must have Silent Bell set to Yes.

Note: Fire and Gas points always function as if this parameter is set to No.

RPS Menu Location

Points > Point Indexes 1-20 > Invisible Point

Buzz On Fault

Default:

– Point Indexes 1-8, 10-20: 0

– Point Index 9: 1

Selections: 0 to 3

This parameter generates 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, Interior Follower)	Operation for Non-Controlled Points (24-Hour)
0	The point buzzes at the keypad only if it enters into the trouble event indicated in Point Response.	Same operation as controlled points.
1	The point generates a Buzz Until Restore at the keypad for any fault event while the point is disarmed. The buzz continues until the point restores and the user acknowledges the event 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 event regardless of the armed state. The buzz continues until the point restores and the user acknowledges the event using a passcode or ENTER key. The point must be normal before the user can silence the buzz.

Selection	Operation for Controlled Points (Part On, Interior, Interior Follower)	Operation for Non-Controlled Points (24-Hour)
2	The point buzzes at the keypad for any fault event 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 event 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 event when the area is disarmed. The user cannot silence this buzz, but it silences automatically when the point is restored. If the fault event results in a trouble response, the keypad continues to buzz even after the user acknowledges the event if the fault is still present.	The point buzzes at the keypad for any fault event regardless of the armed state. The user cannot silence this buzz, but it silences automatically when the point is restored. If the fault event results in a trouble response, the keypad continues to buzz even after the user acknowledges the event if the fault is still present.

RPS Menu Location
Points > Point Indexes 1-20 > Buzz on Fault

Watch Point

Default:
- Point Indexes 1 to 6: No
- Point Indexes 7 to 8: Yes
- Point Indexes 9 to 20: No

Selections:
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.
This parameter allows a controlled point to generate a watch tone as long as the area is disarmed and not being faulted into a trouble or alarm event.
RPS Menu Location
Points > Point Indexes 1-20 > Watch Point

Output Response Type

Default: 0
Selections:

0 Point state does not affect the operation of the corresponding output.

1 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 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.
RPS Menu Location
Points > Point Indexes 1-20 > Output Response Type

Display as Device

Default: No
Selections:
Yes Display [CHECK DEVICE] when this point is off normal.
No Do not display [CHECK DEVICE] when this point is off normal.
Use this parameter to cause the 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 event.
RPS Menu Location
Points > Point Indexes 1-20 > 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 20: No

Selections:
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.
Use this parameter to allow a controlled point to report alarms, troubles and restoral reports only when the area is armed.
Note: 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 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.
This parameter affects keyswitch points and suppresses keyswitch (troubles/restorals).
This parameter does not affect local annunciation.

RPS Menu Location
Points > Point Indexes 1-20 > Local While Disarmed

Local While Armed

Default: No
Selections:
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.
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.
This parameter suppresses all reports from 24-hour points. This parameter only works for disarmed points, and a 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.
RPS Menu Location
Points > Point Indexes 1-20 > Local While Armed

Disable Restorals

Default: No
Selections:
Yes Disable restoral reports for this point.
No Enable restoral reports for this point.
Use this parameter to disable any restoral reports from this point after it returns to normal from an alarm or trouble event.
RPS Menu Location
Points > Point Indexes 1-20 > Disable Restorals

Force Arm Returnable

Default: No
Selections:
Yes This point automatically returns to the system when it restores to normal.
No This point stays out of the system until the area is disarmed.
Use this 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.
RPS Menu Location
Points > Point Indexes 1-20 > Force Arm Returnable

Bypass Returnable

Default: No
Selections:
Yes This point automatically returns to the system when the area is disarmed.
No This point stays out of the system through arming and disarming cycles.
Use this 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.
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.
RPS Menu Location
Points > Point Indexes 1-20 > Bypass Returnable

Bypassable

Default:
– Point Indexes 1 to 7-13, 20: Yes
– Point Index 2-6, 14-19: No
Selections:
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 (Refer to Auto Close), or by a Sked programmed to arm the area.
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 perimeter 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 .
RPS Menu Location
Points > Point Indexes 1-20 > Bypassable

Swinger Bypass

Default: No
Selections:
Yes Enable Swinger Bypass for this point.
No Disable Swinger Bypass for this point.
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 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.

RPS Menu Location

Points > Point Indexes 1-20 > Swinger Bypass

Additional resources

Swinger Bypass Count

Report Bypass at Occurrence

Default: No

Selections:

Yes Send a report at the time that the point is bypassed.

No Do not send a report at the time the point is bypassed.

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. Refer to Defer Bypass Report.

RPS Menu Location

Points > Point Indexes 1-20 > Report Bypass at Occurrence

Defer Bypass Report

Default: No

Selections:

Yes Send a report with the closing report instead of when the point is bypassed by a user.

No Do not defer bypass reports.

Use this parameter to prevent points that are bypassed by the user from reporting 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.
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.

RPS Menu Location

Points > Point Indexes 1-20 > Defer Bypass Report

Cross Point

Default: No
Selections: Yes/No
This parameter reduces false alarms. Points can be programmed so that the control panel needs two faults within a programmed period of time from at least two points within a cross point group before creating cross point alarm events.
Yes Enable cross point alarm events.
No Disable cross point alarm events.

The control panels support the following number of cross point groups:
– B5512: 6 groups
– B4512: 4 groups
– B3512: 2 groups
The Cross Point function is fixed to a minimum of two points per group.
Only use this parameter with Part On, Interior or 24-hour point types with instant alarm response.
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 minimum 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 Responses set to generate 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 event, 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 events. It does not apply to supervisory or trouble events.
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. It is recommended that all points in a cross zone group use the same point index.

Cross Point Group	Point Range
1	1-8
2	9-16
3	17-24
4	25-32
5	33-40
6	41-48

RPS Menu Location
Points > Point Indexes 1-20 > Cross Point

Additional resources
Point Response
Cross Point Timer
Alarm Abort

Alarm Verify

Default:
– Point Indexes 1 to 4: No
– Point Index 5: Yes
– Point Indexes 6 to 20: No

Selections:
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:
– 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 goes into alarm, the control panel removes power to all resettable points for the duration programmed in Restart Time. If the point (or another resettable point in the area) is still in alarm, or goes back into alarm within 65 seconds after the initial verification time reset, an alarm is generated.

Alarm verification points must be programmed as Resettable.

During a Fire Walk Test, the reset time is 5 seconds. The time programmed in Restart Time is ignored.

RPS Menu Location
Points > Point Indexes 1-20 > Alarm Verify

Further Information
Cross Point
Point Type
Resettable
Restart Time

Resettable

Default:
- Point Indexes 1 to 3: No
- Point Indexes 4 to 5: Yes
- Point Indexes 6 to 20: No

Selections:

Yes This point is reset by the RESET SENSORS? function and during the alarm verification sequence.

No This point is not resettable.

Use this parameter if this is a powered point that requires interruption of power to reset a latched alarm event. The resettable point function is typically used with smoke detectors and glass break detectors.

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 sensor restart time (configured in Restart Time), alarms and troubles from these points are ignored. 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.

Do not mix fire and intrusion devices on the same powered loop.

RPS Menu Location

Points > Point Indexes 1-20 > Resettable

Alarm Abort

Default:
- **Point Indexes 1, 7-16:** Yes
- **Point Indexes 2-6, 17-19:** No

Selections:

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.

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.

IMPORTANT: To comply with UL standards, the total amount of time entered in Entry Delay and Alarm Event Abort must not exceed 1 minute.

An alarm is aborted by performing an alarm silence operation before this time elapses at a keypad showing the burglar alarm event. When an alarm is successfully aborted, the keypad shows an optional `ALARM NOT SENT` message. Refer to Abort Display for more information.

This parameter does not apply to fire alarms or invisible point alarms. When upgrading a non- control panel account to a control panel account, RPS forces the default to **No**.

RPS Menu Location

Points > Point Indexes 1-20 > Alarm Abort

Wireless Point Supervision Time

Default: 24 Hours
Selections: None, 4, 12, 24, 48, 72 Hours
This parameter sets the length of time in hours between failure to hear from the wireless transmitter before sending a missing event for devices configured to report to the Wireless Receiver.
None Disable wireless point supervision.
4, 12, 24, 48, 72 Set the length of time in hours for wireless point supervision.
RADION 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.
RPS Menu Location
Points > Point Indexes 1-20 > Wireless Point Supervision Time

Custom Function

Default: Disabled
Selections:
B5512: Disabled, Function 128, Function 129, Function 130, Function 131
B4512: Disabled, Function 128, Function 129
B3512: Disabled, Function 128
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 1-20 > 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) a disarmed control panel waits after a point faults before reporting the event to the central station.
The control panel sends a Burg Supervisory 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 monitor delay at the keypad.
Enable this feature to monitor a door, such as a trash compactor, jewelry case, or freezer that should not be left open.
IMPORTANT
Starting a walk test that includes controlled points, or arming the points' area, will cancel the monitor point timer. No report is sent after the configured time expires.
RPS Menu Location
Points > Point Indexes (point profiles) > Monitor Delay

Delay Response, Disarmed

Default: 00:00
Selections: 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

Perimeter points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using part on 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.
Perimeter points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.
When a Perimeter Point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Perimeter Point trips, the control panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Perimeter Point's entry delay time is less than the remaining time, it shortens the entry delay time.
Perimeter 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 the area All On. They are not armed when using Part On 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 (Refer to 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 (Refer to 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 the area. They are not armed when using part on 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: 00:05 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 perimeter point type with a Point Response of 9 to E. 24-hour points do not show faults when an arming function is entered, but perimeter points do. When programming for this type of protection, you should consider using the Buzz On Fault and Local While Disarmed options.

Hold-up devices in UL installations: the 24-Hour point type must be used for points connected to hold-up devices. The point text must include, “hold-up”.

Part On

Perimeter points are armed with all arming functions. Points programmed as perimeter can also be armed as a group (using part on 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.

Perimeter points can be programmed to initiate entry delay time. If the point initiates entry delay, it can also initiate an entry tone.

When a Perimeter Point is programmed for entry delay, entry delay time is always provided. If the area is in entry delay when a second Perimeter Point trips, the control panel compares the remaining entry delay time to the time programmed for the second Perimeter Point. If the second Perimeter Point's entry delay time is less than the remaining time, it shortens the entry delay time.

Perimeter 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 all on the area. They are not armed when using part on 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 (Refer to 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 (Refer to 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 the area. They are not armed when using part on 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 effect of 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 Schedules

11.1 Open/Close Windows

Open/Close Windows Overview

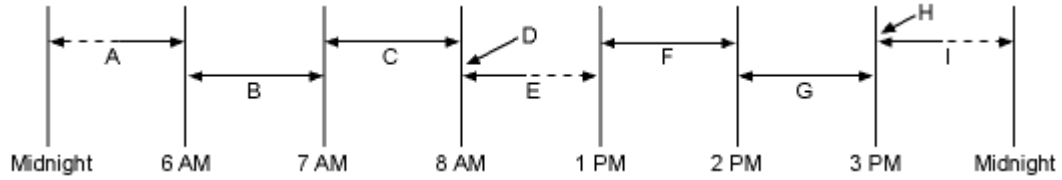
Use these windows to set a schedule for disarming and arming. The disarming and arming schedules provide several independent features:

- 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 parameters and program closing window times.

Opening Window Timeline

Example using two opening windows on the same day



Areas that are disarmed between midnight and 6 AM generate Opening reports.
Areas that are disarmed between 6 AM and 7 AM generate Early to Open reports.
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.
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.
If the user disarms the area between 8:01 AM and 12:59 PM then a Late to Open event is generated.
Areas that are disarmed between 1 PM and 2 PM generate Early to Open reports.
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.
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.
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 / Monday	22:00	23:30	23:59				Yes/**No**	1 2 3 4	**1** 2 3 4 5 6 7 8
2 / Monday	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**

		OPEN			CLOSE			
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

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
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.
RPS Menu Location
Schedules > Open/Close Windows > Sunday through Saturday

Open Early Begin

Default: Disable
Selections: Disable, 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).
– 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.
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.

RPS Menu Location
Schedules > Open/Close Windows > Open Early Begin

Open Window Start

Default: Disable
Selections: Disable, HH:MM (hours and minutes)
This parameter is one of three required to create an opening window. 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).
To program an opening window, Open Early Begin and Open Window Stop must also be programmed.

RPS Menu Location
Schedules > Open/Close Windows > Open Window Start

Additional resources
Open Early Begin
Open Window Stop

Open Window Stop

Default: Disable
Selections: Disable, 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 control 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. Refer to 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.
RPS Menu Location
Schedules > Open/Close Windows > Open Window Stop

Close Early Begin

Default: Disable
Selections: Disable, 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).
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 00:00 start 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.
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.

RPS Menu Location
Schedules > Open/Close Windows > Close Early Begin

Close Window Start

Default: Disable
Selections: Disable, HH:MM (hours and minutes)
This parameter is one of three required to create a closing window. 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).
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.
Refer to Close Early Begin for report feature explanations.
RPS Menu Location
Schedules > Open/Close Windows > Close Window Start

Close Window Stop

Default: Disable
Selections: Disable, HH:MM (hours and minutes)
This parameter is one of three required to create a closing window. 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, 2:45 PM is entered as 14:45).
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. Refer to 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
Yes Do not activate this window on holidays.
No A holiday does not prevent this window from activating.
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.
RPS Menu Location
Schedules > Open/Close Windows > Xept on Holiday
Additional resources
Holiday Indexes for O/C Windows

Holiday 1 (O/C Windows)

Default (Holiday 1): No
Selections:
Yes Use the selected holiday index with this window.
No Do not use the selected holiday index with this window.
This parameter enables 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.
RPS Menu Location
Schedules > Open/Close Windows > Holiday 1

Areas 1-4

Default: No
Selections: Yes/No
Yes Activate the window in the specified area number.
No Disable the window in the specified area number.
This parameter determines whether a particular window activates in each of the control panel's areas.
The B5512 supports up to 4 areas. The B4512 supports up to 2 areas. The B3512 supports 1 area.
RPS Menu Location
Schedules > Open/Close Windows > Areas 1-4

11.2 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. Refer to 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.

User Group

Default: 1
Selections: 0, 1, 2, 3, 4
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.
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.
RPS Menu Location
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.

RPS Menu Location

Schedules > User Group Windows > Sunday through Saturday

Additional Information

Xept Holiday

Group Enable Time

Default: Disable

Selections: Disable, HH:MM (hours and minutes)

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.

IMPORTANT: This parameter must be programmed if this User Group Window is assigned to a user group.

Make entries using a 24-hour clock (for example, 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.

RPS Menu Location

Schedules > User Group Windows > Group Enable Time

Group Disable Time

Default: Disable

Selections: Disable, HH:MM (hours and minutes)

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.

IMPORTANT: This parameter must be programmed if this user group window is assigned to a user group.

Make entries using a 24-hour clock. For example, 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.

RPS Menu Location

Schedules > User Group Windows > Group Disable Time

Xept Holiday (User Group 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. Use the instructions provided in Xept Holiday .

RPS Menu Location

Schedules > User Group Windows > Xept Holiday

Holiday 1

Default: No
Selections: Yes/No
Yes Use the selected holiday index with this window.
No Do not use the selected holiday index with this window.
This parameter enables 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.
RPS Menu Location
Schedules > User Group Windows > Holiday 1
or Schedules > Skeds > Holiday 1

11.3 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.
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 parameter.
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 (Refer to 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.
RPS Menu Location
Schedules > Skeds > Sked Descriptions

11.3.1 Sked 1-5

Time Edit

Default: Yes
Selections:
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.

Select whether the user can edit the time of this Sked from the keypad.

RPS Menu Location

Schedules > Skeds > Time Edit

Function

Default: Send Test Report

Selections: See list of Sked functions below.

Select the function name from the drop down list that you want this Sked to execute. RPS 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. Selections in the Parameter 1: Area # prompt 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.

– B5512 Arm Area allows entries up to 4 areas in Parameter 1: Area#
– B4512 Arm Area allows entries up to 2 areas in Parameter 1: Area#
– B3512 Arm Area allows entries up to 1 area in Parameter 1: Area#

All On Instant

This function simulates the All On Instant keypad function. Entries in the Parameter 1: Area # field 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.

– B5512 Arm Area allows entries up to 4 areas in Parameter 1: Area#
– B4512 Arm Area allows entries up to 2 areas in Parameter 1: Area#
– B3512 Arm Area allows entries up to 1 area in Parameter 1: Area#

Part On Delay

This function simulates the Part On Delay keypad function. Selections in the Parameter 1: Area # prompt 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.

– B5512 Arm Area allows entries up to 4 areas in Parameter 1: Area#
– B4512 Arm Area allows entries up to 2 areas in Parameter 1: Area#
– B3512 Arm Area allows entries up to 1 area in Parameter 1: Area#

Part On Instant

This function simulates the Part On Instant keypad function. Selections in the Parameter 1: Area # prompt 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.

– B5512 Arm Area allows entries up to 4 areas in Parameter 1: Area#
– B4512 Arm Area allows entries up to 2 areas in Parameter 1: Area#
– B3512 Arm Area allows entries up to 1 area in Parameter 1: Area#

Disarm

This function emulates the Disarm keypad function. Selections in the Parameter 1: Area # prompt define the area(s) this Sked disarms. The Sked can disarm multiple areas.

- B5512 Disarm Area allows entries up to 4 areas in Parameter 1: Area#
- B4512 Disarm Area allows entries up to 2 areas in Parameter 1: Area#
- B3512 Disarm Area allows entries up to 1 area 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 2. 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 Point keypad function. The entry in the Parameter 1: Point # prompt defines the point this Sked bypasses. The point can be bypassed only if Bypassable is programmed YES in the Point Index assigned to the point. The bypass is reported if 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 Point keypad function. The entry in the Parameter 1: Point # 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. Selections in the Parameter 1: Area # prompt define 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.

- B5512 Unbypass Individual Point allows entries up to 4 areas in Parameter 1: Area#
- B4512 Unbypass Individual Point allows entries up to 2 areas in Parameter 1: Area#
- B3512 Unbypass Individual Point allows entries up to 1 area in Parameter 1: Area#

Turn Output On

This function emulates the Change Output keypad function to turn outputs ON. The entry in the Parameter 1: Output # field defines the specific output this Sked activates. The Sked can activate one output.

Turn Output Off

This function emulates the Change Output keypad function to turn outputs OFF. The entry in the Parameter 1: Output # field defines the specific output this Sked disables. The Sked can disable 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 Parameter 1: Output # field 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.

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 Report 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 Parameter 1: Deferred 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.

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.

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.

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 selected in Parameter 1: Area #. 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 selected in Parameter 1: Area #. 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 for the keypads selected in Parameter 1: Keypad #. 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 selected in Parameter 1: Keypad #. The Watch Tone sounds at all Keypads with the address programmed. Press ESC to silence the tone.

Select up to 8 keypads.

Set Keypad Volume

This function sets the configured keypads shown in Parameter 1: Keypad # to the volume level entered in Parameter 2: Volume Level. Refer to Keypad Volume in the keypad configuration section for details on volume parameters.

Set Keypad Brightness

This function sets the configured keypads shown in Parameter 1: Keypad # to the brightness level selected in Parameter 2: Brightness Level. Refer to the Keypad Brightness parameter in the keypad configuration section for details on the brightness parameter.

Execute Custom Function

This function executes the custom function selected in Parameter 1: Custom Function # at a scheduled time.

RPS Menu Location

Schedules > Skeds > Function

Time

Default: Disable

Selections: Disable, HH:MM (hours and minutes)

Enter the time that the Sked executes using a 24-hour clock (for example, 2:45 PM is entered as 14:45).

Disabled Skeds displays "Disabled"in the cell.

Follow these steps to program a time:

1. Double-click on the field corresponding to the Sked you wish to program the time for.
2. If "Disable" is checked, uncheck it. The time field will become active.

3. Click inside the time field and either use the up and down arrows to set the time, or type in the desired time.
4. 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.

RPS Menu Location

Schedules > Skeds > Time

Date

Default: Disable
Selections: Disable, Day/Month (ex. 12 June)
Enter the date that the Sked executes. Disabled Skeds display "Disabled" in the Date cell.

RPS Menu Location

Schedules > Skeds > Date

Sunday through Saturday (Skeds)

Default (Sunday through Saturday): No
Selections: Yes/No
These seven day of the week parameters select the days of the week that the Sked is active.
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.

RPS Menu Location

Schedules > Skeds > Sunday through Saturday

Xept on Holiday (Skeds)

Default: No
Selections: Yes/No

Yes Prevent this Sked from operating on the Holidays identified in the specific Holiday Index(es) used with this Sked. Specific Holiday Indexes are selected in this programming section and programmed in the next programming module.

No This Sked operates on Holidays programmed in the Holiday Index(es) used with this Sked.

If no Days of the Week are programmed, this Sked operates only on the Holidays programmed in the Holiday Index(es) used with this Sked. This Sked also operates if the Holiday falls on a day of the week that is programmed.

RPS Menu Location

Schedules > Skeds > Xept on Holiday

Holiday 1

Default: No
Selections:
Yes Use the selected holiday index with this window.
No Do not use the selected holiday index with this window.
This parameter enables 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.
RPS Menu Location
Schedules > User Group Windows > Holiday 1
or Schedules > Skeds > Holiday 1

11.4 Holiday Indexes

Holiday Indexes Schedule

This parameter sets 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 appears. 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, 2012, is set as a holiday, October 24 will be a holiday in 2013, 2014, and so on. But the holiday will fall on different days of the week.
RPS Menu Location
Schedules > Holiday Index > Holiday Indexes Schedule

12 Automation

Automation Device

Default: None
Selections:
– **None** Automation communication is disabled.
– **Mode 1** using onboard connection without TLS
– **Mode 1** using B426 module at SDI2 address 1
– **Mode 1** using onboard connection with TLS
– Mode 2 using onboard connection or B426 module at SDI2 address 1, TLS or secure UDP connection

This parameter enables and selects the communication module to use exclusively for automation communication.
RPS Menu Tree Location:
Automation > Automation Device

Status Rate

Default: 0
Selections: 0 - 255
This parameter sets how often the default status information is sent to the Serial Interface Module.
0 Status information never sent *unless requested*.
1 – 255 Status information is sent at the interval programmed.
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, 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. 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.
RPS Menu Tree Location
Automation > Status Rate

Automation Passcode

Default: Bosch_Auto
Selections: 0-24 characters
This parameter sets the passcode that must be entered before automation software can connect to the control panel.
Enter up to 24 characters with no spaces. The password is case-sensitive. The automation passcode must be entered before any other automation commands are accepted by the control panel.
RPS Menu Tree Location

Automation > Automation Passcode

Application Passcode

Default: Bosch_RSC
Selections: 6-24 characters
Use this parameter to configure the password the panel must receive from a remote device to establish a secure connection (smart phone with Bosch RSC is an application example).
Enter between 6 to 24 characters with no spaces. The passcode is case sensitive. The application passcode must be entered before any other commands from the remote device are accepted by the control panel.
RPS Menu Tree Location:
Automation > Application Passcode

Mode 1 Automation Ethernet Port Number

Default: 7702
Selections: 1 to 65535
This parameter sets the port number for the Mode 1 Automation Ethernet.
RPS Menu Tree Location:
Automation > Mode 1 Automation Ethernet Port Number

13 SDI2 Modules

13.1 B208 Octo-input

B208 Octo-input Information

The B208 Octo-input is a device that attaches to the SDI2 bus of the control panel. Each module provides 8 independently monitored control loops.

Capacity

Panel type	Modules supported
B5512	4
B4512	2
B3512	0

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 Enable Enclosure Tamper.
No Disable Enclosure Tamper.
This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.
RPS Menu Location
SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

13.2 B308 Octo-output

B308 Octo-output Information

The B308 Octo-output is a device that attaches to the SDI2 bus of the control panel. It provides 8 independently controlled outputs similar in function to those provided by the output modules

Capacity

Panel type	Modules supported
B5512	5
B4512	3
B3512	0

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

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes Enable Enclosure Tamper.
No Disable Enclosure Tamper.
This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.
RPS Menu Location
SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

13.3 IP Communicator

IP Communicator Information

Connecting a B426
1. The B426 should be connected to the SDI2 bus.
2. Set the B426's rotary switch to Address 1.
3. Connect the B426 to the control panel.

Configuring a B426
When installing a B426 Ethernet Communication Module it is important to make sure that the available configuration parameters are set properly to insure proper module operation.
The B426 Ethernet Communication Module is used to connect to the control panel over an Ethernet network. Typical uses include PC front-end (automation) software packages, network RPS connection for off-site programming, diagnostic troubleshooting, 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
B5512	1
B4512	1
B3512	1

You can use one or both communication modules for central station reporting or RPS communications. Optionally, you can use one of the B426 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 module takes effect after RPS disconnects from the control panel.
- If the B426 is configured through the B426 configuration web interface to disable control panel programming (that is, **Panel Programming Enable** is set to No), then RPS programming of the B426 is accepted by the control panel, but not applied to the B426. The **Panel Programming Enable** parameter is not available in RPS.

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes Enable Enclosure Tamper.
No Disable Enclosure Tamper.
This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.

RPS Menu Location

SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

IPv6 Enable

Default: No
Selections:
Yes Enable IPv6.

No Disable IPv6 (IPv4 mode being used).

This parameter sets which mode is being used.
When IPv6 Enable is set to Yes:

– IPv4 parameters are Read Only.
– The IPv4 address, IPv4 subnet mask, and IPv4 Default Gateway are locked (i.e. grayed out and not editable).
– The DHCP/AutoIP enable should be set to Yes.

When IPv6 Enable is set to No, IPv6 parameters are Read Only.

RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Enable
SDI2 > IP Communicator > IPv6 Enable

IPv4 DHCP/AutoIP Enable

Default: Yes
Selections:

Yes Enable DHCP to automatically configure the IP Address, IP Default Gateway, and IP DNS Server Address.

No Manually configure the Onboard Ethernet Communicator. Use this setting if there is no DHCP service.

This parameter configures the Onboard Ethernet communicator automatically using DHCP
DHCP allows a computer to be automatically configured which eliminates the need for interaction by a network administrator. DHCP also provides a central database that tracks computers that connect to the network, which prevents two computers from accidentally being configured with the same IP address.
AutoIP enables dynamic IP addresses to be assigned to a device when the device is started up. DHCP requires a DHCP server.
When Yes is selected, the IPv4 address, IPv4 Subnet Mask, and IPv4 Default Gateway are grayed out and cannot be changed.
When No is selected, IPv6 Mode should be set to No.
Note: If IPv6 Enable is set to Yes, then this option is not available. The parameter has no effect on B450 operation.

RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DHCP/AutoIP Enable
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 Ethernet communication method if DHCP is disabled.
If IPv4 DHCP/Auto IP Enable is not selected than this must be configured.
The IPv4 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 of 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:

Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 address
SDI2 Modules > IP Communicator > IPv4 address

IPv4 Default Gateway

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
This parameter configures the address of the local network gateway to the Internet or Intranet.
A gateway is a point on a TCP/IP network that serves as an entrance to another network. A host uses a default gateway when an IP packet's destination address belongs to someplace outside the local subnet. The default gateway address is usually an interface belonging to the LAN's border router. In DHCP mode, the default gateway is usually resolved automatically. When DHCP/AutoIP Enable is set to Yes, this parameter cannot be changed. Leave the default value.
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Default Gateway
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.
A Domain Name Server (DNS) converts internet domain names or hostnames 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 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.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DNS server IP address
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:FFFF: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 hostnames to their corresponding IP addresses. In DHCP mode, the default value indicates that 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 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 Locations

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DNS server IP address
SDI2 Modules > IP Communicator > IPv6 DNS server IP address

UPnP (Universal Plug and Play) Enable

Default: Yes
Selections:
Yes Enable IP devices to connect on the network.

No Disable IP devices from connecting on the network.

This parameter allows IP devices to discover each other's presence on the network and connect for communication. This parameter also allows a router to forward port numbers through the keypad itself, allowing reports to reach receivers behind the router.
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > UPnP (Universal Plug and Play) Enable
SDI2 Modules > IP Communicator > UPnP (Universal Plug and Play) Enable

HTTP Port Number

Default: 80
Selections: 1 to 65535
This parameter allows the configuration of the web server port number.
When TLS Enhanced Security is enabled, HTTPS is applied. The default value for HTTPS is 443. If enhanced security is not enabled, the HTTP value is applied.
The parameter has no effect on B450 operation.
RPS Menu Location
SDI2 Modules > IP Communicator > HTTP Port Number.

ARP Cache Timeout

Default: 600
Selections: 1 to 600 (seconds)
This parameter specifies the time-out for ARP cache entries (time-out value in seconds).
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > ARP Cache Timeout
SDI2 Modules > IP Communicator > ARP Cache Timeout

Web/USB Access Enable

Default: No
Selections: Yes/No
This parameter enables authorized users to view and modify the B426 configuration parameters using an Internet 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: blank, 4-10 case sensitive alphanumeric characters
Use this parameter to set the password required to log in for web access. Characters can be a combination of letters and numbers. The password is case sensitive. Blank space will disable the password checking.
RPS Menu Location
SDI2 > IP Communicator > Web/USB Access Password

Firmware Upgrade Enable

Default: No
Selections: Yes/No
This parameter enables the control panel to modify the module's firmware through an external Web interface.
Yes Modify the firmware through the web interface.
No Modify the firmware through 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)
This parameter allows the user to customize a module hostname. This is the hostname that represents the communication device on the network.
Optionally, use the hostname to contact the control panel via RPS over network, for Remote Security Control, or for module web configuration and diagnostics.
IMPORTANT
– If this field is left blank, Ethernet communicator module will determine its hostname based on its MAC address (the factory default hostname).
– Use the hostname on a local network using DHCP. To use the hostname externally, enter the hostname in the DNS server.
The parameter has no effect on B450 operation.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Module Hostname
SDI2 Modules > IP Communicator > Module Hostname

Unit Description

Default: Blank
Selections: Up to twenty alphanumeric characters.
This parameter describes the B426 module (location, attributes, etc.) shown in the configuration pages..
The parameter has no effect on B450 operation.
RPS Menu Location
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 is typically configured as 7700 when the control panel is communicating with the B5512, B4512 and B3512, a central station receiver, RPS, or Automation. 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.
RPS Menu Location
SDI2 Modules > IP Communicator > TCP/UDP Port Number

TCP Keepalive Time

Default: 45
Selections: 0 - 65 (seconds)
This parameter sets 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.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > TCP Keepalive Time
SDI2 Modules > IP Communicator > TCP Keepalive Time

IPv4 Test Address

Default: 8.8.8.8
Selections: IPv4 address or Domain Name
This parameter sets the IPv4 Test Address. The IPv4 Test Address is used by the Onboard Ethernet communicator connection to ping an internet address in order to verify the integrity of the network and the network configuration setting.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Test Address
SDI2 Modules > IP > IPv4 Test Address
Additional resources:
Network Address Format

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 Onboard Ethernet communicator 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
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Test Address
SDI2 Modules > IP Communicator > IPv6 Test Address
Additional resources:

Network Address Format

Web and Automation Security

Default: Enable
Selections:
Disable Enhanced security is not applied.
Enable Enhanced security is applied.
This parameter enables enhanced security for Automation and B426 Web Access. 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.
RPS Menu Location
SDI2 > 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 an alternate IPv4 DNS server IP address.
If the module fails to obtain an address from the primary server, the alternate DNS server is used if one has been specified. The Alternate 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 Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv4 DNS server IP address
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.
The Alternate 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 has a value between 0000-FFFF. When this is defined through the DHCP service, leave the default value. If the module fails to obtain an address from the primary server, the Alternate IPV6 DNS server is used, if specified. The module can use the Alternate IPv6 DNS server only when the Primary address is not the default address.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv6 DNS server IP address
SDI2 > IP Communicator > Alternate IPv6 DNS server IP address

13.3.1 B450 Cellular

IMPORTANT CELLULAR SERVICE INFORMATION

Refer to Configuring for Cellular Communication for important information regarding how to set up your control panel to ensure proper cellular communication with the central station receiver.

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
Panel Wide Parameters > Cellular Plug-in Module > Inbound SMS
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inbound SMS
Additional Information
Conf iguring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Session Keep Alive Period
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Session Keep Alive Period
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Inactivity Timeout
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Inactivity Timeout

Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Low Signal Strength
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Low Signal Strength

Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for No Towers
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for No Towers

Additional Information
Configuring for Cellular Communication

Reporting Delay for Single Tower

Default: 0
Selections:

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

Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Single Tower
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Reporting Delay for Single Tower

Additional Information

Configuring for Cellular Communication

Outgoing SMS Length

Default: 160

Selections:

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

Panel Wide Parameters > Cellular Plug-in Module > Outgoing SMS Length
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Outgoing SMS Length

Additional Information

Configuring for Cellular Communication

13.3.1.1 Cellular GPRS

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
Panel Wide Parameters > Cellular Plug-in Module > SIM PIN
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > SIM PIN
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point User Name
SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point User Name
Additional Information
Configuring for Cellular Communication

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
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Password

SDI2 Modules > IP Communicator > B450 Bus Device Cellular > Cellular GPRS > Network Access Point Password

Additional Information

Configuring for Cellular Communication

13.4 B520 Aux Power Supply

B520 Auxiliary Power Supply Information

The B520 Auxiliary Power Supply is a device that attaches to the SDI2 bus of the control panel. It provides a supervised 12 Volt DC 2.5 Amp auxiliary power supply. Each power supply might support 2 separate 12V nominal lead acid batteries with a capacity of 7-18 Ah.

Capacity

Panel type	Modules supported
B5512	4
B4512	2
B3512	1

Settings

RPS supports the configuration of the Enclosure Tamper on each of the Power Supply modules. **Yes** = Enable enclosure tamper, **No** = Disable enclosure tamper. Default setting is No.

RPS supports the configuration of the Module Enable on each of the Power Supply modules. **Yes** = Enable module supervision, **No** = Disable module supervision. Default setting is No.

RPS supports the configuration of the One or Two batteries on each of the Power Supply modules.

Switch Settings

Ref. Hardware Switch Settings > SDI2 Devices > B520 Power Supply Switch Settings

Module Enable

Default: No

Selections: Yes or No

Yes Supervise the SDI2 module.

No Do not supervise the SDI2 module.

This parameter indicates to the control panel if the SDI2 module should be supervised.

RPS Menu Location

SD12 > B520 Power Supply > Module Enable

Module Enclosure Tamper

Default: No

Selections: Yes or No

Yes Enable Enclosure Tamper.

No Disable Enclosure Tamper.

This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.

RPS Menu Location

SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

One or Two Batteries

Default: One
Selections: One or Two
This parameter specifies if 1 or 2 backup batteries are installed with the Auxiliary Power Supply module.

Menu Tree Location

SDI2 Modules > B520 Aux Power Supply > One or Two Batteries

13.5 Wireless Receiver

Wireless Receiver Information

The B820 Inovonics SDI2 Wireless Interface Module is supported on the SDI2 bus of the control panel. It provides the ability to use wireless key fobs, repeaters and points with the 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.

Settings

RPS supports the configuration of the Enclosure Tamper on each of the Wireless Receiver modules. **Yes** = Enable enclosure tamper, **No** = Disable enclosure tamper. Default setting is No
RPS supports the configuration of the global System Supervision Time for devices configured to report to the Wireless Receiver.
RPS supports the configuration of the Low Battery Resound on each of the Wireless Receiver modules.

Switch Settings

Refer to B810/B820 Wireless Receiver Switch Settings

Wireless Module Type

Default: B810 RADION Wireless
Selections:
– Unassigned
– B810 RADION Wireless
– B820 Inovonics Wireless
This parameter identifies the wireless device
Unassigned No Point Source is able to be set to Wireless.
B810 RADION Wireless There is no limit on how many Point Source options can be set to Wireless. The RADION wireless module can support up to 1800 devices.
B820 Inovonics Wireless The control panel is limited to 350 wireless devices not including repeaters.
Reference
Panel Wide Parameters > SDI2 Modules > Wireless Receiver > Wireless Module Type

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes Enable Enclosure Tamper.
No Disable Enclosure Tamper.
This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.
RPS Menu Location
SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

System Supervision Time

Default: 12 Hours
Selections: None, 4, 12, 24, 48, 72 hours
None Disable wireless device supervision.
4, 12, 24, 48, 72 hours Specify the length of time in hours between hearing from the Wireless receiver before sending a missing event.
RPS supports the configuration of the global System Supervision Time. 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.
Note: Inovonics keyfobs are not supervised when assigned to a user.
All fire points are fixed at a 4 hour supervision time regardless of the System Supervision Time setting.
RPS Menu Location
SDI2 > Wireless Receiver > System Supervision Time

Low Battery Resound

Default: Never Resound
Selections: Never Resound, 4, 24 hours
This parameter is global for all non-fire points. The control panel will automatically fix the Low Battery Resound at 24 hours for fire points. RPS supports the configuration of the Low Battery Resound on the wireless repeater modules.
Reference
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

13.6 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 wireless interface module be configured as part of the system.

Module Enclosure Tamper

Default: No
Selections: Yes or No
Yes Enable Enclosure Tamper.
No Disable Enclosure Tamper.
This parameter sets 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 tamper is opened, or removed from its mounting location. RPS supports the configuration of the Enclosure Tamper on each of the wireless receiver modules.
RPS Menu Location
SDI2 > B208 Octo-input > Module Enclosure Tamper
SDI2 > B308 Octo-output > Module Enclosure Tamper
SDI2 > IP Communicator > Module Enclosure Tamper
SDI2 > B520 Aux Power Supply > Module Enclosure Tamper
SDI2 > Wireless Receiver > Module Enclosure Tamper
SDI2 > Wireless Repeater > Module Enclosure Tamper

RFID (B820 Inovonics Wireless)

Default: N/A
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
Selection: 0 - 99999999
This parameter provides a unique way for the Wireless Receiver and Wireless Repeaters to identify what device is transmitting.
The **R**adio **F**requency device **Identification** number (RFID) 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)

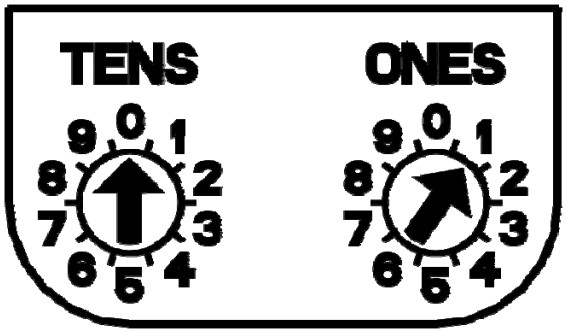
14 Hardware Switch Settings

B91x Keypad Assignments

		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

B92x/B93x Keypad Assignments

Set the address switches per the control panel configuration. If multiple SDI2 keypads reside on the same system, each SDI2 keypad must have a unique address. For single-digit addresses 1 through 9, set the tens switch to 0. The following example shows the address switch setting for address 1.



KP#	Address #	Tens	Ones
KP 1	Address 1	0	1
KP 2	Address 2	0	2
KP 3	Address 3	0	3
KP 4	Address 4	0	4
KP 5	Address 5	0	5
KP 6	Address 6	0	6
KP 7	Address 7	0	7
KP 8	Address 8	0	8

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.
The B5512 supports Points 01 to 48 and modules 1-4.
The B4512 supports Points 01 to 28 and modules 1-2.
The B3512 does not support the B208 Octo-input module.
Terminate unused B208 inputs with an EOL resistor.

B208 Switch Setting	B4512 Point Range	B5512 Point Range
1	11 - 18	11 - 18
2	21 - 28	21 - 28
3		31 - 38
4		41 - 48

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.
The B5512 supports outputs 1 to 58 and modules 1 - 5.
The B4512 supports outputs 1 to 38 and modules 1 - 3.
The B3512 does not support the B308 Octo-output module.

B308 Switch Setting	B3512 Output Range	B4512 Output Range	B5512 Output Range
1	n/a	11 - 18	11 - 18
2	n/a	21 - 28	21 - 28
3	n/a	31 - 38	31 - 38
4	n/a		41 - 48
5	n/a		51 - 58

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 Switch Setting	Address	Bus Type	Function
0			Local Configuration setting (default setting)
1	1 (173)	SDI2	Automation or RPS, Reporting

B520 Power Supply Switch Settings

The rotary address switch range for the B520 is between 1 and 4 for the B5512, between 1 and 2 for the B4512 and 1 for the B3512. Address ranges 00 and 05-99 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

B820 Inovonics Wireless Receiver Switch Settings

The B820 Inovonics 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 B Series control panels.

B810 RADION Wireless Receiver Switch Settings

B810 and B820 address switches provide a single-digit setting for the module's address. The module uses address 1. Addresses 0 and 2 through 9 are invalid.
Only address 1 is valid for the B Series control panels.

15 Recommended supervision configuration

To optimize data used for supervision, we recommend the following system settings:

Installation Type	Commercial Burg (UL1610)	High Supervision	Hourly	Medium Security or Household Fire	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

16 Configuring for cellular communication

1. **Setup a cellular account with Bosch.**

An up-to-date Bosch Cellular contract is required before you can order or activate SIM cards or a Plug-in Cellular Communicator. Refer to www.BoschCellular.com or contact your sales representative for details.

After you establish a cellular account, refer to the Cellular Communication Options table below to determine which parameters need to be set in RPS to ensure proper communication between the control panel and the central station receiver.

		Communication Options						
Parameter Location within RPS	**Required Parameters**	**On-board IP**	**Cellular**	**On-board IP w/ Cellular backup**	**Cellular w/ On-board IP backup**	**Personal Notifications**	**VPN**	**Cellular Callback**
System Configuration (one-time settings)								
Cellular Tab	Web Service Details		X	X	X	X	X	X
	Callback IP Address							X
VPN Tab	Add Existing VPN						X	
Panel View (per account)								
Cellular Tab	Cellular Connectivity		X	X	X	X	X	X
	Data Plan Selection		X	X	X	X		
Panel Wide Parameters (per account)								
Cellular Plug-in	Inbound SMS							X
Communicator	Primary Path Device	OIP	CIP	OIP	CIP			
	Backup Path Device			CIP	OIP			
	RG Same			X	X			

		Communication Options						
	Network Receiver							
	Personal Notification					X		
Personal Notification	Personal Notification					X		
Enhanced Communication	Network Address, Port	X	X	X	X			
	Poll Rate, Ack, Retry	X	X	X	X			

OIP = Onboard IP CIP = Cellular IP

2. **Enable the RPS PC to configure and manage cellular services.**

Configure RPS for Cellular or VPN service. This is a system wide configuration and only needs to be setup once.

Config > System

- **Cellular tab.** Configure this tab to enable web services to look up SIM or radio information and manage assigned service plans from within RPS. Credentials for web services are provided in a Bosch Cellular welcome email and can be found in the online service management portal. For RPS initiated cellular without a VPN, this tab configures a Cellular Callback address for the panel to reach an RPS with a public internet address that must be forwarded to a fixed RPS workstation.
- **VPN tab.** Configure this tab if you will connect from the internet to the panel using cellular IP over a PPTP VPN (a login is provided with Bosch Cellular). This one-time setup will automate a PPTP VPN login and connection from within the Connect window in RPS. The VPN client (or Windows VPN) must be setup on your PC before RPS can use it. This setup is not required if your network is configured for always-on IPSec VPN connection to the network provider.

For instructions on setting up Windows VPN, refer to the Bosch Cellular Services User Guide located at http://www.conettix.com/Downloads.aspx.

3. **Configure the control panel account for cellular communication.**

The parameters specified in the Cellular Communication Options table under Panel Data - View and Panel Wide Parameters need to be set for each panel account.

Panel Data - View >

- **Cellular Tab.** Using the SIM or radio MEID number, this tab will retrieve and store the assigned IP address, phone number and assigned plan. Use this screen to select and set an appropriate plan to avoid overage fees.

Panel Wide Parameters >

- **Cellular Plug-in Module.** Default settings should only be changed for high security UL1610 commercial listed installations requiring low signal notification.
- **Communicator.** Select the route group for cellular reporting as primary or backup. Personal Notification routes are also selected here. Note: Route Group 4 is defaulted with more end-user oriented reports but reports can be customized for

any route group. Be sure reporting settings align with texts included in your selected monthly cellular plan.

- **Personal Notification.** Setup descriptions and contact information to be routed in Communicator section.
- **Enhanced Communication.** Set reporting destinations, and polling/supervision settings here. Be sure cellular polling rates follow recommended settings and align with your selected cellular plan.

17 Index

Bosch Security Systems, Inc.
130 Perinton Parkway
Fairport, NY 14450
USA
www.boschsecurity.com