Control Panel

B6512

en Program Entry Guide

Table of contents

1 Remote Programming Software

Remote Programming Software (RPS) is an account management and control panel programming utility for Microsoft Windows operating systems. Operators can perform remote programming, account storage, remote control, and diagnostics for specific control panels.

Support

Access our **support services** at www.boschsecurity.com/xc/en/support/.
Bosch Security and Safety Systems offers support in these areas:

- Apps & Tools
- Building Information Modeling
- Warranty
- Troubleshooting
- Repair & Exchange
- Product Security

Bosch Building Technologies Academy

Visit the Bosch Building Technologies Academy website and have access to **training courses, video tutorials** and **documents**: www.boschsecurity.com/xc/en/support/training/

2 Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

- General information: https://www.boschsecurity.com/xc/en/support/product-security/
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

3 Compliance Settings

3.1 SIA CP-01 Verification

Default: No

Selections:

– Yes - RPS examines the settings for the panel account parameters for SIA CP-01 compliance.

– No - RPS does not examine parameters for compliance.

RPS checks the following parameters for SIA CP-01 compliance:

Duress Type, page 79
Alarm Bell, page 135
Exit Delay Time, page 97
Burg Time, page 103
Exit Delay Warning, page 109
Entry Delay Warning, page 109
Entry Delay, page 206
Passcode Length, page 83
Remote Warning, page 84
Swinger Bypass Count, page 84
Cancel Reports, page 80
Two Man Rule?, page 101 ?
Early Ambush?, page 102?
All On Instant, page 167
Part On Instant, page 167
Passcode Enter Function, page 116

RPS Menu Location

Compliance Verification > SIA CP-01 Verification

3.2 ULC Compliance

Default: No

Selections:

– Yes. Adjust control panel operation for UL Canada (ULC) compliance.

– No. Do not adjust for ULC compliance.

Setting this parameter to Yes configures the control panel to disregard input from all sensors for a minimum of 120 seconds at system start-up.

When sensor processing is started, the control panel reports a unique event prior to reporting any point events. Additionally, no power-induced events are reported unless it is determined that the fault will not be restored within the 120 second delay time.

RPS Menu Location

Compliance Settings > ULC Compliance

3.2.1 CAN/ULC-S304 compliance

CAN/ULC-S304, SIGNAL RECEIVING CENTRE AND PREMISE BURGLAR ALARM CONTROL UNITS

This Standard covers construction and performance requirements for control units and accessories for intrusion alarm systems, including protected premises control units and accessories for local or signal receiving centre connections, and signal receiving centre alarm receiving equipment, including recording equipment. The equipment is intended for use in premises, safes and vaults.

Control panel programming requirements

Setting the ULC Compliance parameter to Yes is the one control panel programming requirement for compliance with the CAN/ULC-S304 standard.

3.2.2 CAN/ULC-S559, required programming

CAN/ULC-S559, Standard for Equipment for Fire Signal Receiving Centres and Systems

CAN/ULC-S559 covers requirements for fire signal receiving centres and systems, which include transmitting and receiving equipment, proprietary fire receiving centre equipment and control unit accessories. Fire signal receiving centre systems include protected premise unit and receiver for ordinary (non-hazardous) indoor and outdoor locations. Programming methods, test, service and other software intended for use with the equipment for fire signal receiving centres and systems are included in the evaluation of the equipment. Signal receiving units used in fire signal receiving centres, satellite centres, signal processing centres and bridging centres are also covered by the requirements in this Standard.

COMPLIANCE SETTINGS > UL Canada Compliance

Set the COMPLIANCE SETTINGS > UL Canada Compliance parameter to Yes.

PANEL WIDE PARAMETERS > Report Routing

In the Route Group 4 column:

- Set Fire Reports, Gas Reports, Burglar Reports, Personal Emergency Reports, User Reports, and Test reports to No.
- Set Output Reports, Auto Function Reports, RPS Reports, Point Reports, User Change Reports, and Access Reports to No.
- Verify Diagnostic Reports is set to Custom. The next steps configure the Custom settings.

PANEL WIDE PARAMETERS > Report Routing > Fire Reports > Fire Cancel

Set the PANEL WIDE PARAMETERS > Report Routing > Fire Reports > Fire Cancel parameter for each Route Group (1 to 4) to No.

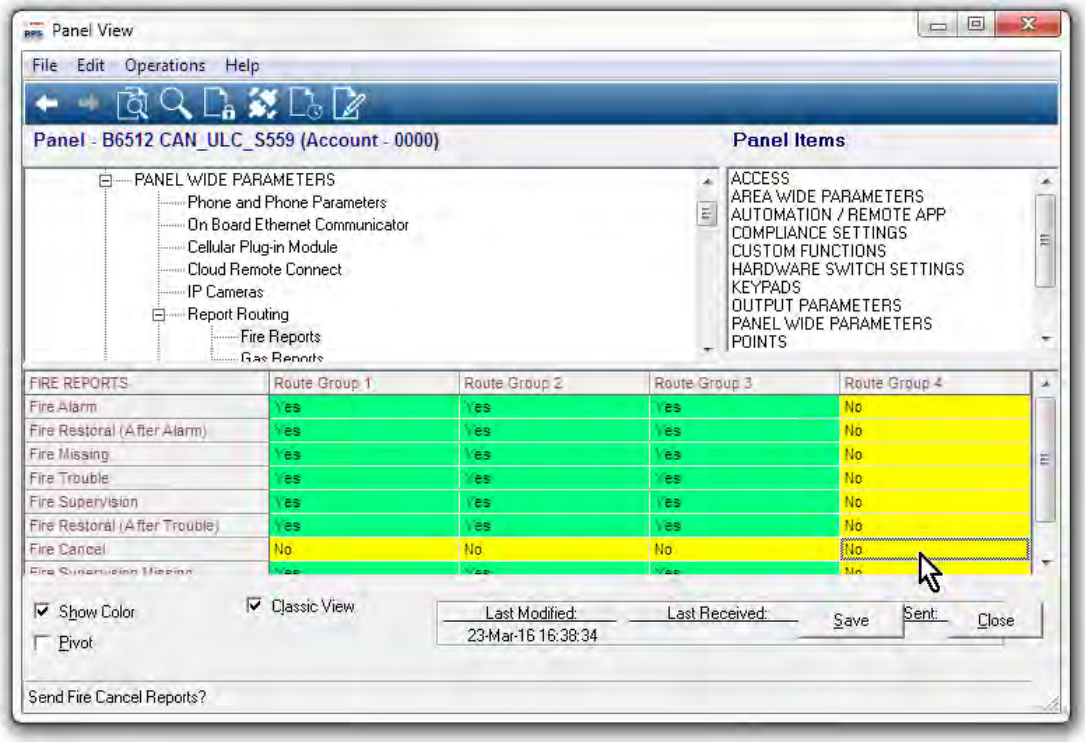


Figure 3.1: Fire Cancel

PANEL WIDE PARAMETERS > Report Routing > Diagnostic Reports

For the Route Group 4 column, set SDI2 Device Failure to Yes. Set the remaining reports to No.

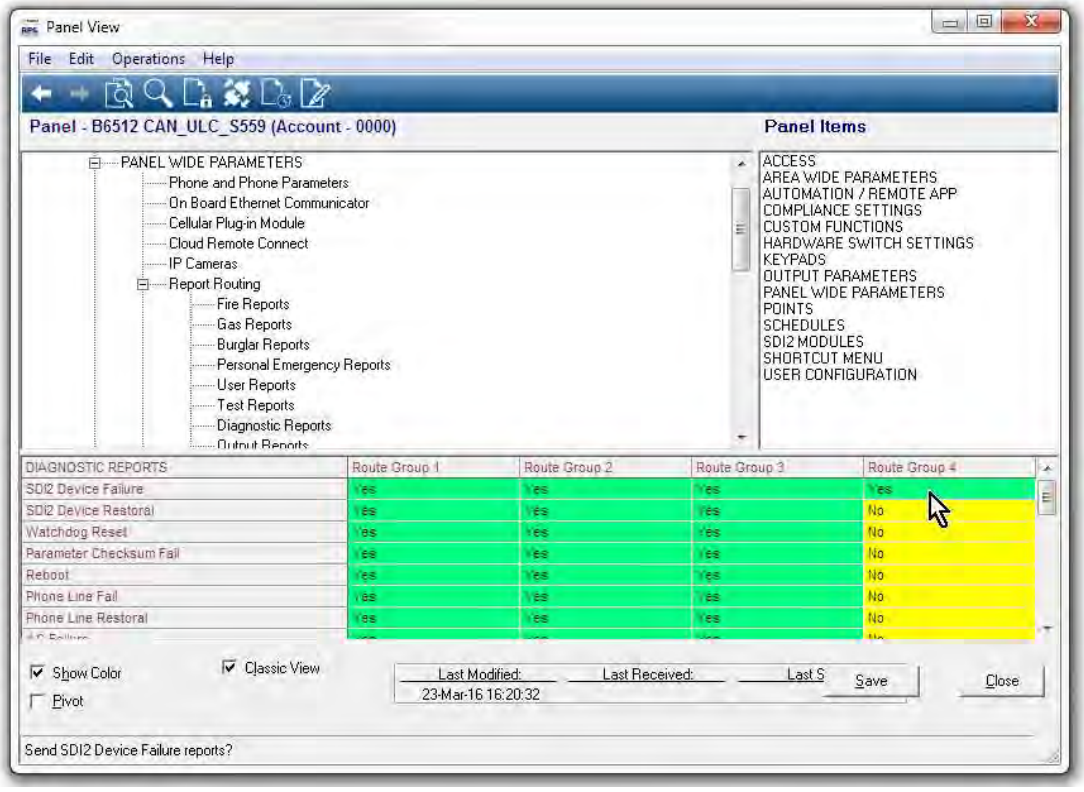


Figure 3.2: SDI2 Device Failure

PANEL WIDE PARAMETERS > Communicator > Primary Destination Device

For the Route Group 4 column, set Primary Destination Device to Destination 4 for the type of device in use (for example, Onboard IP, Destination 4 if the control panel sends reports using the on-board Ethernet.

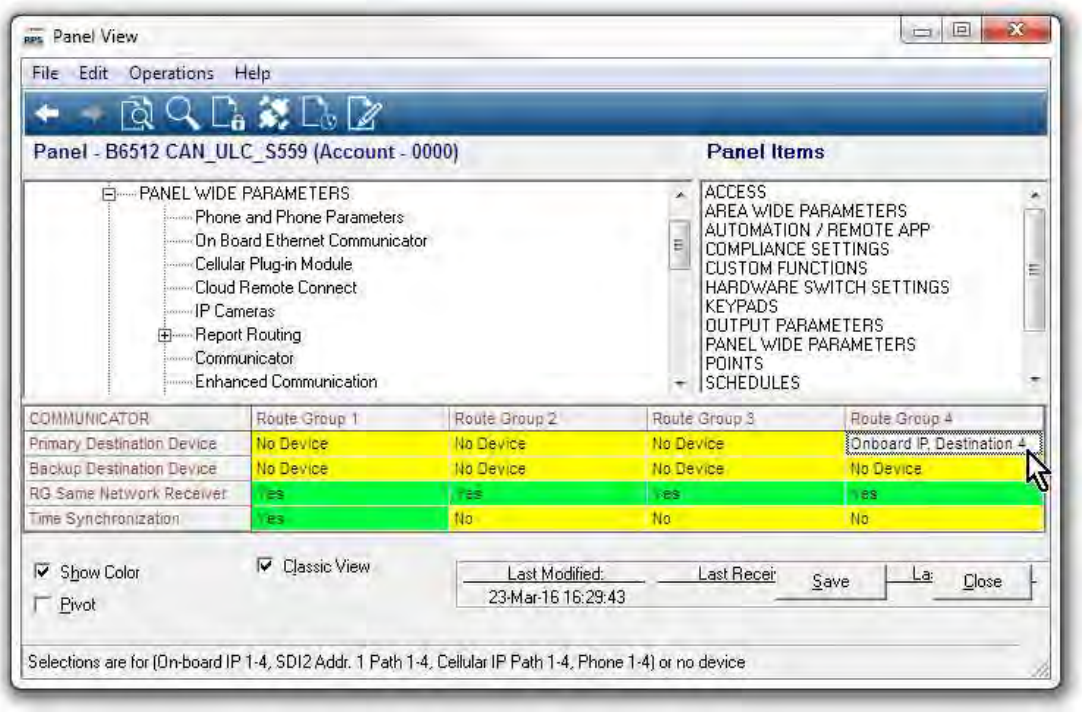


Figure 3.3: Primary Destination Device

PANEL WIDE PARAMETERS > Enhanced Communication > Destination 4

In the Destination 4 column, set Network Address to: 0.1.1.1 (this address is intentionally not a real address on the network). Set the Poll Rate to 0. Set the ACK Wait Time (sec.) to 5.

POINTS > Point Profiles (Point Indexes)

Configure Point Profiles 1, 4, and 6 as shown below.
It is important to configure the parameters in order.

Point Profile 1

Set Alarm Abort to: No.
Set Point Profile Text (First Language) to: Fire Panel Trouble.
Set Point Type / Response / Circuit Style > Point Type to: Fire Point.
Set Point Type / Response / Circuit Style > Circuit Style to: Single EOL (1KΩ) or Single EOL (2KΩ).
Set Response to: 3.

Point Profile 4

Set Point Profile Text (First Language) to: Fire Panel Alarm.
Set Point Type / Response / Circuit Style > Point Type to: Fire Point.
Set Point Type / Response / Circuit Style > Circuit Style to: Single EOL (1KΩ), Single EOL (2KΩ), or Dual EOL.
If you set Point Type / Response / Circuit Style > Circuit Style to Single EOL (1KΩ) or Single EOL (2KΩ), set Response to: 1.
If you set Point Type / Response / Circuit Style > Circuit Style to Dual EOL, set Response to: 0.

Point Profile 6

Set Point Profile Text (First Language) to: Fire Panel Supervisory.
Set Point Type / Response / Circuit Style > Point Type to: Fire Point.
Set Point Type / Response / Circuit Style > Circuit Style to: Single EOL (1KΩ), Single EOL (2KΩ), or Dual EOL.
If you set Point Type / Response / Circuit Style > Circuit Style to Single EOL (1KΩ) or Single EOL (2KΩ), set Response to: 9.
If you set Point Type / Response / Circuit Style > Circuit Style to Dual EOL, set Response to: 2.

Figure 3.4: Point Profiles

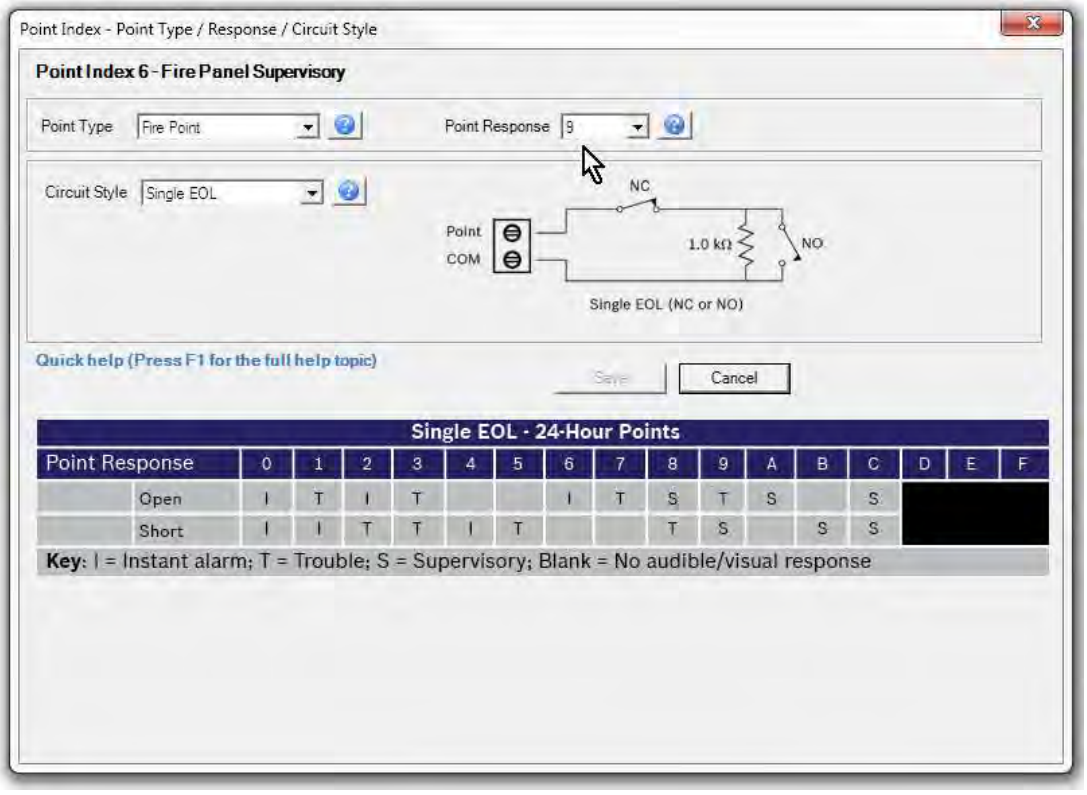


Figure 3.5: Point Type Response and Circuit Style

POINTS > Point Assignments

Set the POINTS > Point Assignments, Text and Profile parameters, for on-board points 1, 2, and 3 as follows.

Point 1

Set Point Assignments > Text to: Fire Panel Alarm.
Set Point Assignments > Profile to: 4 - Fire Panel Alarm

Point 2

Set Point Assignments > Text to: Fire Panel Trouble.
Set Point Assignments > Profile to: 1 - Fire Panel Trouble

Point 3

Set Point Assignments > Text to: Fire Panel Supervisory.
Set Point Assignments > Profile to: 6 - Fire Panel Supervisory

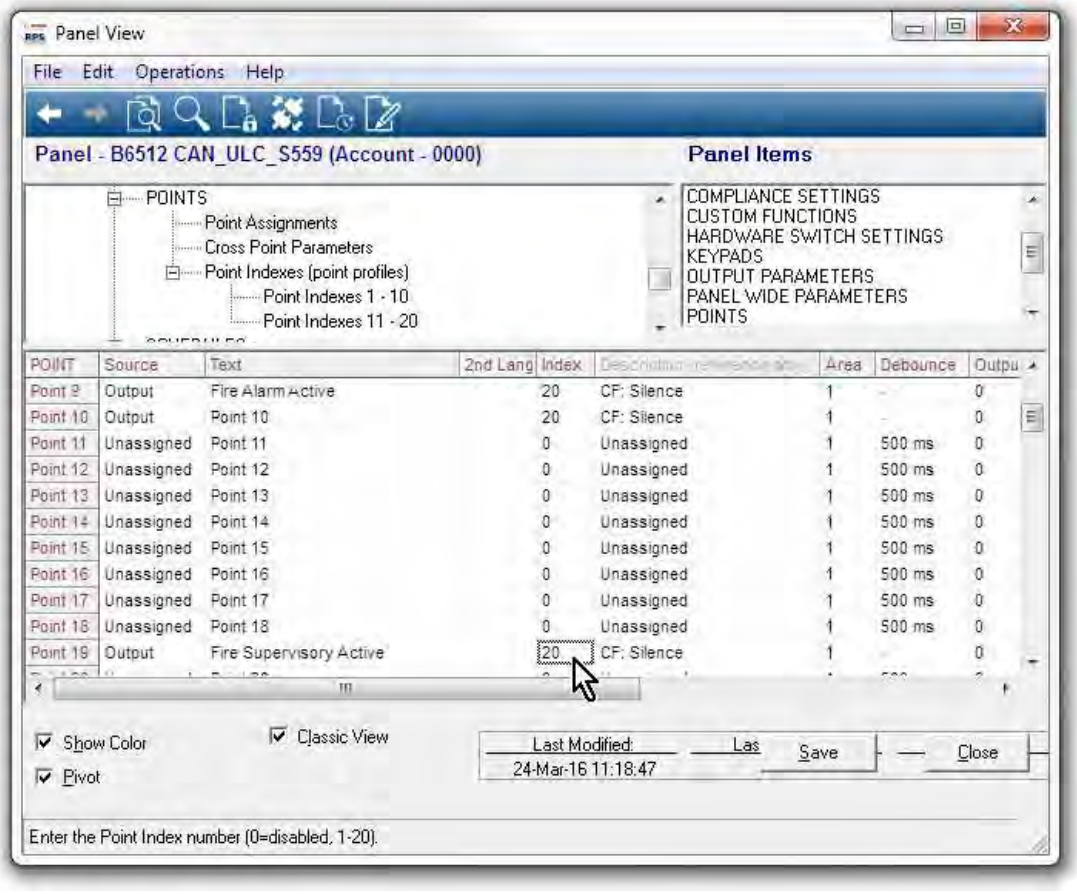


Figure 3.6: Fire Panel Supervisory

3.2.3 CAN/ULC-S559, recommended programming

Control panel silencing of fire alarm panel alarm, trouble, and supervisory events

When control panels are configured as described below, they automatically silence keypads connected to the control panel for fire, trouble, and supervisory events from the fire panel.

CUSTOM FUNCTIONS > Custom Function 128

Set Custom Function 128 > Custom Function Text to: Silence.

Set Custom Function 128 > Function 1 to: Trouble Silence (set Parameter 1 to: Area 1).

Set Custom Function 128 > Function 2 to: Alarm Silence (set Parameter 1 to: Area 1).

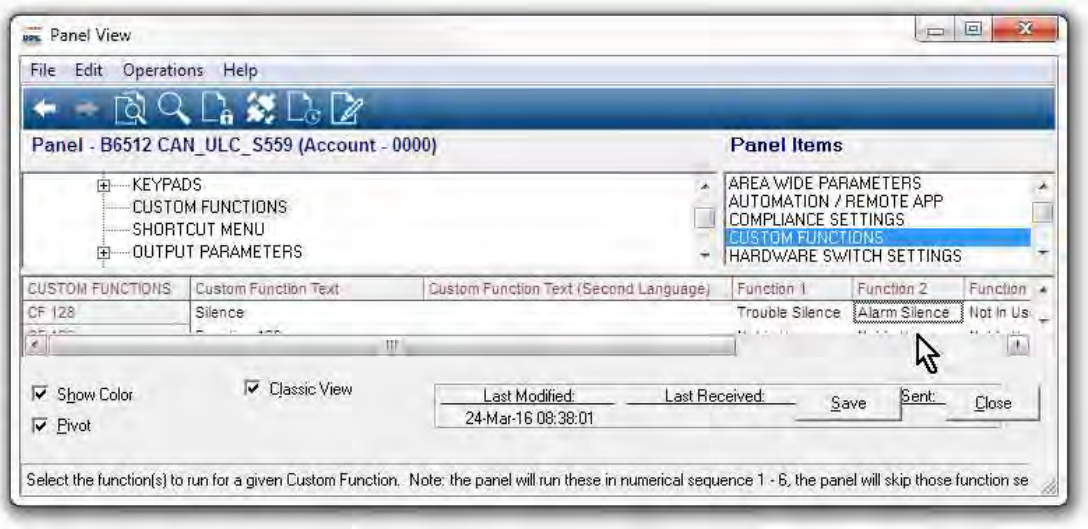


Figure 3.7: Custom Function 128

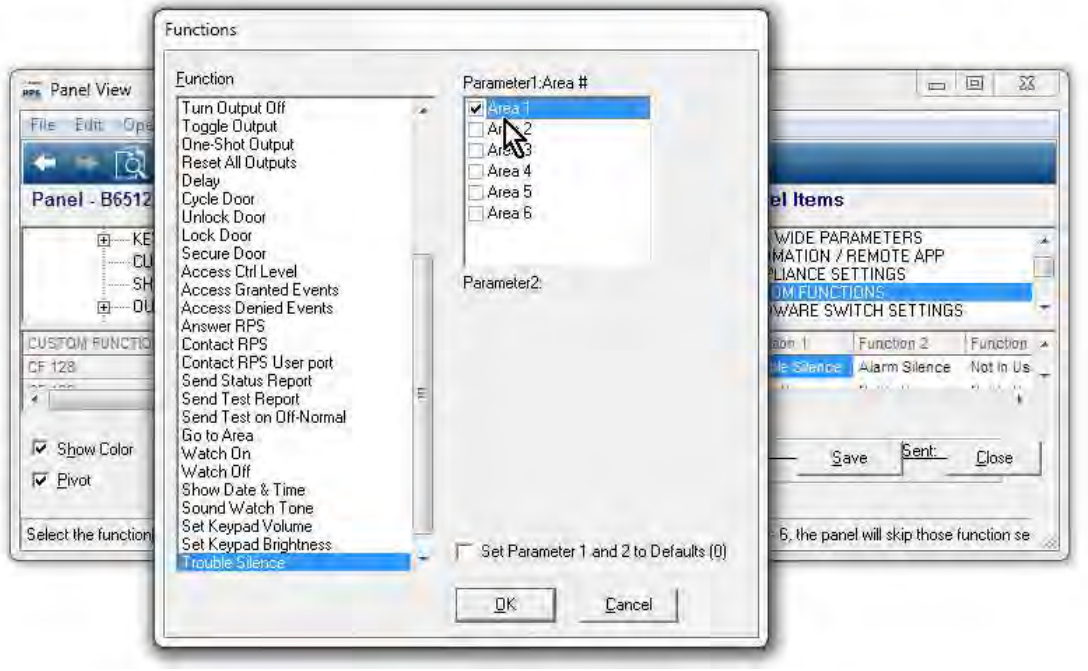


Figure 3.8: Area 1 selection

OUTPUT PARAMETERS > Panel Wide Outputs

For virtual outputs:

Set Panel Wide Outputs > Summary Fire to: 9.

Set Panel Wide Outputs > Summary Fire Trouble to: 10.

Set Panel Wide Outputs > Summary Supervisory Fire to: 19.

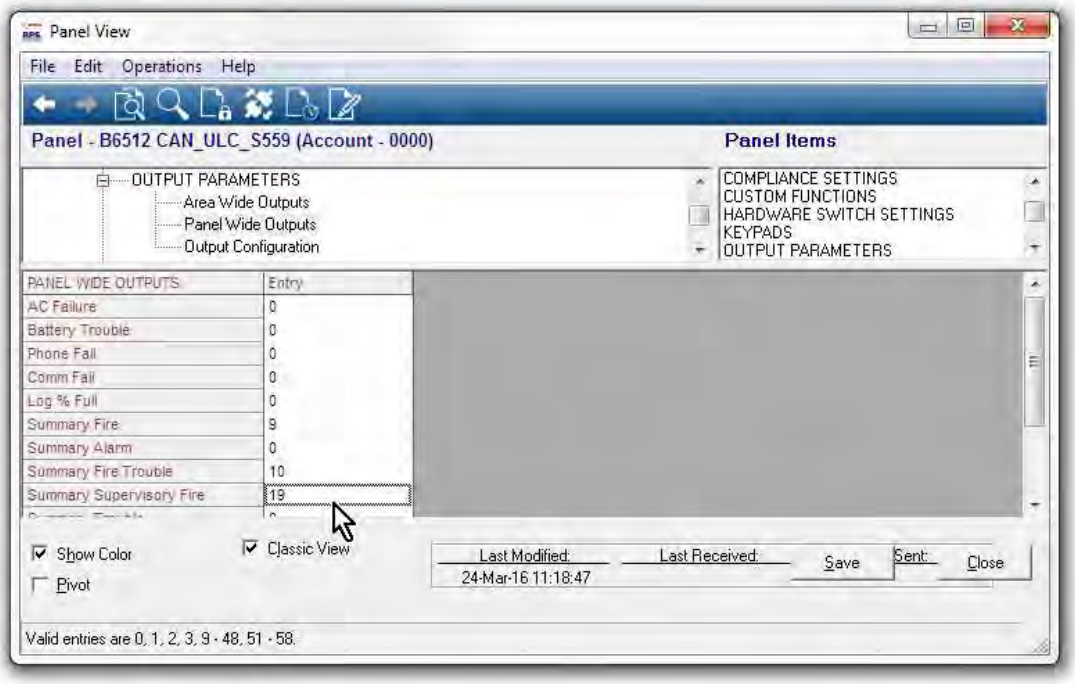


Figure 3.9: Panel Wide Outputs

POINTS > Point Profiles (Point Indexes)

Configure Point Profile 20 as shown below.

It is important to configure the parameters in order.

Point Profile 20

Set Point Profile Text (First Language) to: CF: Silence.

Set Point Type / Response / Circuit Style > Point Type to: Custom Function.

Leave Point Type / Response / Circuit Style > Circuit Style at the default: Single EOL (1KΩ).

Leave Point Type / Response / Circuit Style > Response at the default: 7.

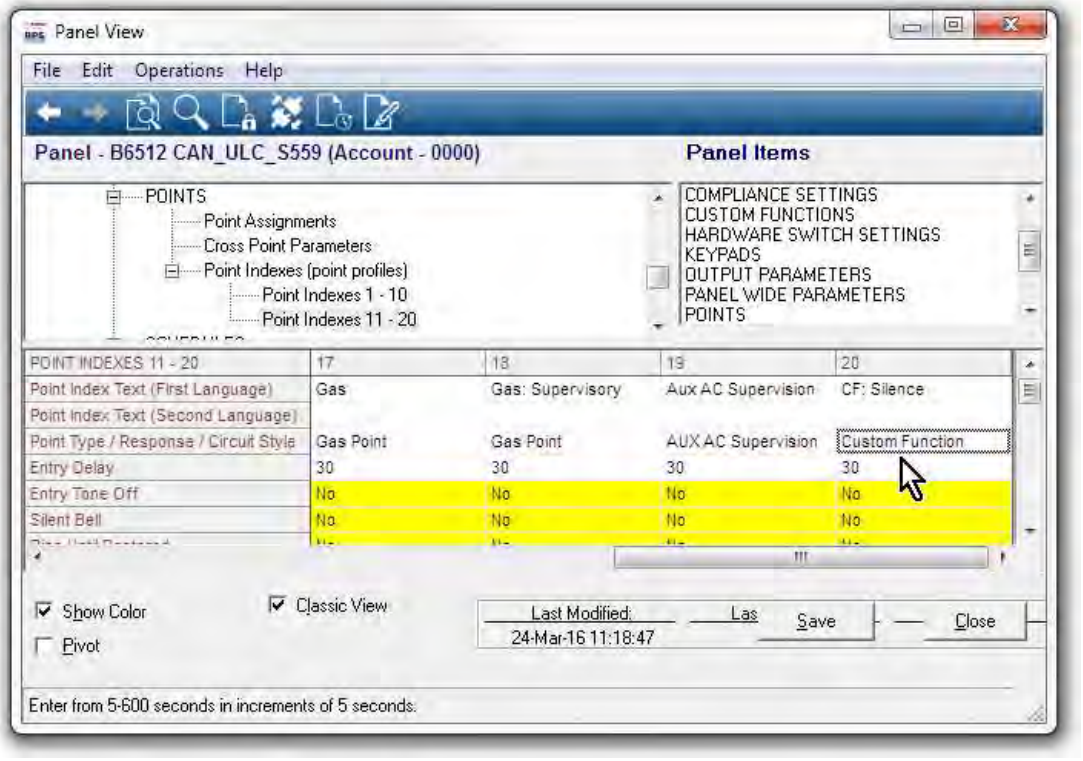


Figure 3.10: Point Profile 20

POINTS > Point Assignments

Set the POINTS > Point Assignments, Source, Text, and Profile parameters, for points 9, 10, and 19 as follows.

Point 9

Set Point Assignments > Source to: Ouput.
Set Point Assignments > Text to: Fire Alarm Active.
Set Point Assignments > Profile to: 20 - CF: Silence

Point 10

Set Point Assignments > Source to: Ouput.
Set Point Assignments > Text to: Fire Trouble Active.
Set Point Assignments > Profile to: 20 - CF: Silence

Point 19

Set Point Assignments > Source to: Ouput.
Set Point Assignments > Text to: Fire Supervisory Active.
Set Point Assignments > Profile to: 20 - CF: Silence

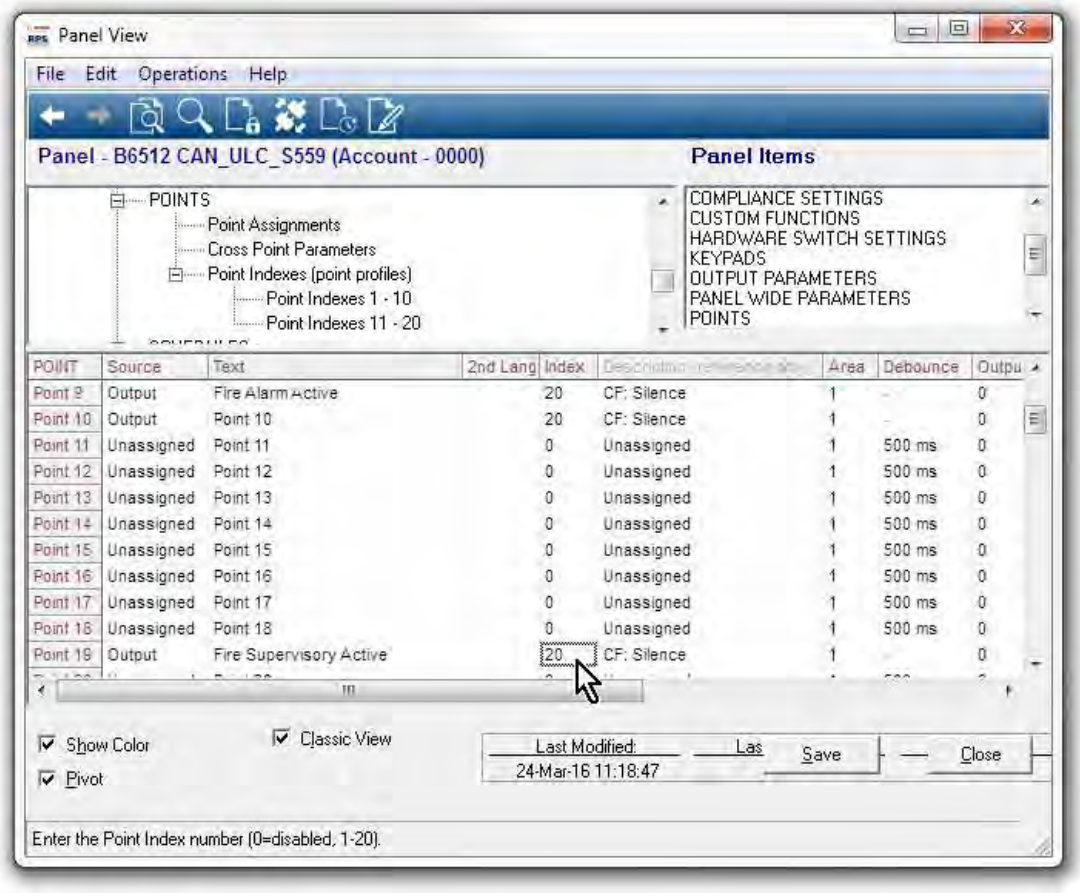


Figure 3.11: Point Assignments

3.3 Supervision configuration

Optimizing data used for supervision:

Installation Type	Commercial Burg (UL1610)	Commercial Burg (ULC S304)	High Supervision	Hourly	Medium Security or Household Fire	Daily Supervision
Required Supervision Interval	200 sec	180 sec	300 sec	1 hr	4 hr	25 hr
Recommended Service Plan	Extended	Extended	High Supervision	Standard	Standard	Backup
Panel Programming						
Receiver Supervision Time	200 sec	Custom	300 sec	1 hr – NFPA	4 hr – Medium Security	25 hr
Panel Poll Rate (sec)	n/a	89 sec	n/a	n/a	n/a	n/a

Installation Type	Commercial Burg (UL1610)	Commercial Burg (ULC S304)	High Supervision	Hourly	Medium Security or Household Fire	Daily Supervision
Panel ACK Wait (sec)	n/a	15	n/a	n/a	n/a	n/a
Panel Retry Count	n/a	5	n/a	n/a	n/a	n/a

3.4 European application

Default: No

Selections:

Yes - European market application. SIA DC-09 communicator format will be available for use.
No - Not a European market application. SIA DC-09 communicator format will not be available for use.

Notice!

SIA DC-09 has not been investigated for use by UL and will not be available for non-European applications. Do not select the SIA DC-09 communicator format for any UL or ULC applications.

RPS Menu Location

Compliance Settings > European Application

4 Panel Wide Parameters

4.1 Phone and Phone Parameters

4.1.1 Phone Destination 1 (to 4)

Default: Blank

Selections:

- Blank - the control panel dials no phone number.
- 0-9 - the control panel dials these characters.
- C - the control panel pauses 2 seconds when it sees a C in the dialing sequence.
- D - the control panel dials when it detects dial tone, or when the initial 7-second dial tone detect period expiries. To extend the dial tone detect period, insert D at the beginning of the dialing sequence.
- #,* - the control panel dials these characters as if they were pressed on a telephone keypad.

Enter the dialing sequence (telephone number) the control panel uses to send reports to the central station receiver.

Leaving this parameter blank does not disable the Phone Destination. To prevent use of the phone destination, do not assign it to a Primary or Backup Destination Device. For more information, refer to *Communicator, overview, page 63*.

Configuring Phone Destinations for Call Waiting

Dialing a call waiting sequence on a non-call waiting line prevents the control panel from successfully sending reports to the central station receiver. If a customer cancels call waiting service without notifying their security company, the control panel is unable able to send reports using the Backup Destination Device.

If you configure a Phone Destination with a phone number that includes a sequence to cancel call waiting, choose that Phone Destination as the *Primary Destination Device, page 65* for a Route Group. Configure another Phone Destination without the call waiting cancel sequence and choose it as the *Backup Destination Devices, page 66* for the Route Group.

RPS Menu Location

Panel Wide Parameters > Phone and Phone Parameters > Phone Destination 1 to 4

4.1.2 Phone Destination 1 (to 4) Format

Default: Modem4

Selections:

- Modem4 - the control panel sends expanded Modem4 reports to the central station receiver. Expanded information includes point text, output text, and user names.
- Contact ID - the control panel sends Contact ID reports. Use this format when the central station receiver does not support the Modem4 format.

RPS Menu Location

Panel Wide Parameters > Phone and Phone Parameters > Phone Destination (1 to 4) Format

4.1.3 DTMF Dialing

Default: Yes

Selections:

- Yes - the control panel dials phone numbers using DTMF (dual-tone multi-frequency, touch-tone).
- No - the control panel dials phone numbers using pulse dialing.

Before setting this parameter to No, make sure the PSTN (Public Switched Telephone Network) the control panel is connected to supports pulse dialing.

RPS Menu Location:

Panel Wide Parameters > Phone and Phone Parameters > DTMF Dialing

4.1.4 Phone Supervision Time

Default: 0

Selections:

– 0 - disabled, no phone line supervision.

– 10-240 (seconds) - number of seconds (in 10 second increments) a phone line must be faulted before the control panel creates a phone line fail event.

The control panel does a phone line check approximately nine times a minute. If it detects a fault on the phone line that lasts the number of seconds set at this parameter, it creates a phone line fail event.

Keypads show a phone line fail and make a trouble tone if the *Buzz on Fail, page 32* and *Trouble Tone, page 118* parameters are set to Yes. If the *Alarm on Fail, page 32* parameter is set to Yes, keypads show an alarm event and make an alarm tone.

When the phone line is normal (fault is cleared) for the number of seconds set at this parameter, the control panel creates a phone line restoral event.

The control panel sends phone line fail and phone line restoral reports when the events occur. They are also included in *Expand Test Report, page 33*.

Phone line fail events are assigned to Area 1 and use the Area 1 configuration.

RPS Menu Location

Panel Wide Parameters > Phone and Phone Parameters > Phone Supervision Time

4.1.5 Alarm on Fail

Default: No

Selections:

– Yes - alarm response (burg bell, keypad alarm tone, alarm report) for phone line fail events.

– No - no alarm response for phone line fail events

To use this Alarm on fail feature, enable phone line supervision at the Phone Supervision Time parameter.

Refer to *Phone Supervision Time, page 32*.

The alarm response for phone line fail events includes:

– activating the Area 1 Burglar Bell,

– activating the alarm tone at keypads

– sending alarm reports

RPS Menu Location

Panel Wide Parameters > Phone and Phone Parameters > Alarm on Fail

4.1.6 Buzz on Fail

Default: No

Selections:

– Yes - panel-wide trouble tone at all keypads when a phone line fail event occurs.

– No - no trouble tone at any keypad when a phone line fail event occurs.

To use this Buzz on fail feature, set phone line supervision at the Phone Supervision Time parameter.

Refer to *Phone Supervision Time, page 32*.

Panel-wide trouble tones are set for individual keypads at the Trouble Tone parameter (*Trouble Tone, page 118*). The default for the Trouble Tone parameter for all keypads is No (no trouble tone for panel wide troubles).

RPS Menu Location

Panel Wide Parameters > Phone and Phone Parameters > Buzz On Fail

4.1.7 Expand Test Report

Default: No

Selections:

– Yes - expand user test reports and sked (scheduled) test reports to include off-normal system status information.

– No - Do not expand test reports.

When this parameter is set to Yes, the test report (or test off-normal report) is followed by a diagnostic report for each off-normal system status. Refer to Panel Wide Parameters > Report Routing > *Diagnostic Reports, page 59* for a list of reports included.

Notice!

Expanded Test Report set to Yes

When the Expanded Test Report is set to **Yes**, you must set the reporting format to **Modem4**.

RPS Menu Location

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

4.1.8 PSTN Compatibility

Default: Appropriate value for region

Selections:

Algeria	El Salvador	Lebanon	Reunion
Argentina	Equador	Lesotho	Romania
Armenia	Estonia	Liechtenstein	Russia
Australia	Finland	Lithuania	Saudi Arabia
Austria	France	Luxembourg	Singapore
Bahamas	Georgia	Macao	Slovakia
Bahrain	Germany	Malaysia	Slovenia
Belarus	Ghana	Malta	South Africa
Belgium	Greece	Martinique	Spain
Bermuda	Guadeloupe	Mexico	Sri Lanka
Brazil	Guam	Moldova	Sweden
Brunei	Hong Kong	Morocco	Switzerland
Bulgaria	Hungary	Netherlands	Taiwan
Canada	Iceland	New Zealand	Thailand
Caribbean	India	Nigeria	Tunisia
Chile	Indonesia	Norway	Turkey
China	Ireland	Oman	UAE
Colombia	Israel	Pakistan	Ukraine
Costa Rica	Italy	Paraguay	United Kingdom
Croatia	Japan	Peru	Uruguay
Cyprus	Jordan	Philippines	USA
Czech Republic	Kazakhstan	Poland	Uzbekistan

Denmark	Korea	Polynesia (French)	Venezuela
Dominican Republic	Kuwait	Portugal	Yemen
Dubai	Kyrgyzstan	Puerto Rico	Zambia
Egypt	Latvia	Qatar	

This parameter configures the control panel and the B430 Plug-in Telephone Communicator for public switched telephone networks (PSTN).

Notice!
PSTN requirement for Australia / New Zealand, disable RPS answer armed/disarmed
If you set this PSTN Compatibility parameter to Australia or New Zealand, you must set Panel Wide Parameters > RPS Parameters > Answer Armed and Answer Disarmed to 0 (disabled).

RPS Menu Location
Panel Wide Parameters > Phone and Phone Parameters > PSTN Compatibility

4.2 On Board Ethernet (IP) Communicator

4.2.1 IPv6 Mode

Default: No
Selections:
– Yes - use IPv6 mode (Internet Protocol version 6) for IP communications
– No - use IPv4 mode (Internet Protocol version 4) for IP communications

When IPv6 Enable is set to Yes, set DHCP/AutoIP enable to Yes.
When IPv6 Enable is set to No, the IPv6 parameters are grayed out (no access to them).
When IPv6 Enable is set to Yes, The IPv4 parameters are grayed out (no access to them).
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Mode,

4.2.2 IPv6 DHCP

Default: Enabled (Yes)
Selections:
– Enabled (Yes) - DHCP automatically sets the IP Address, IP Default Gateway, and IP DNS Server Address. AutoIP enables dynamic IP addresses to be assigned to devices at start-up.
– Disabled (No) - Set this parameter to Disabled if there is no DHCP service. Manually set the IP Address, IP Default Gateway, and IP DNS Server Address.

DHCP requires a DHCP server.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DHCP

4.2.3 IPv4 DHCP/AutoIP Enable

Default: Enabled (Yes)
Selections:
– Enabled (Yes) - DHCP automatically sets the IP Address, IP Default Gateway, and IP DNS Server Address. AutoIP enables dynamic IP addresses to be assigned to devices at start-up.

– Disabled (No) - Set this parameter to Disabled if there is no DHCP service. Manually set the IP Address, IP Default Gateway, and IP DNS Server Address.

DHCP requires a DHCP server.
When this parameter is set to Yes, the IPv4 address, IPv4 Subnet Mask, and IPv4 Default Gateway are grayed out. You cannot change them.
When the IPv6 Mode parameter is set to Yes, this parameter is grayed out (no access to it).

RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DHCP/AutoIP Enable

4.2.4 IPv4 Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).
If IPv4 DHCP/Auto IP Enable is set to No, enter the IPv4 address here.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Location
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 address

4.2.5 IPv4 Subnet Mask

Default: 255.255.255.0
Selections: 0.0.0.0 to 255.255.255.255
If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).
If IPv4 DHCP/Auto IP Enable is set to No, enter the IPv4 sub-network mask here.
The control panel uses the subnet mask to more efficiently identify the network and node parts of the address.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Subnet Mask

4.2.6 IPv4 Default Gateway

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).
If IPv4 DHCP/Auto IP Enable is set to No, enter the Default Gateway address here.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Default Gateway4 Default Gateway

4.2.7 IPv4 DNS Server IP Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
A Domain Name Server (DNS) uses internet domain names or hostnames to supply corresponding IP addresses. In DHCP mode, the DHCP server's default DNS is used. To use a custom DNS server in DHCP mode, enter the custom DNS server's IP address here.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 DNS server IP address

4.2.8 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 sets the IPv6 DNS server address for Static IP mode.
When this address is set by the DHCP service, do not change it.
A Domain Name Server (DNS) uses internet domain names or hostnames to supply corresponding IP addresses. In DHCP mode, the DHCP server's default DNS is used. To use a custom DNS server in DHCP mode, change the parameter to the custom DNS server's IP address.
This IPv6 DNS server address is the only IPv6 address entered as numbers.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 DNS server IP address

4.2.9 UPnP (Universal Plug and Play) Enable

Default: Yes
Selections:
Yes (Enabled) – use UPnP to open a port forwarder for inbound RPS and RSC (Remote Security Control) connections
No (Disabled) – do not use UPnP
The UPnP parameter has no effect on event reporting to a central station receiver.
When this parameter is set to Yes, the control panel sends a request to the premises router to open a port forwarder. The port forward allows inbound RPS and RSC (Remote Security Control) connections.

Notice!
UPnP requires IP Address / Host Name and Panel Port
In the Panel Data – View, Network tab, make sure the IP Address / Host Name and Panel Port parameters are entered.

RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > UPnP (Universal Plug and Play) Enable

4.2.10 ARP Cache Timeout (seconds)

Default: 600
Selections: 1 to 600 (seconds)
This parameter specifies the time-out for ARP cache entries.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > ARP Cache Timeout

4.2.11 Module Hostname

Default: Blank

Selections: 1-63 characters, a-z, A-Z, 0-9, hyphen (-) in the 0000.0000.0000.0000 format. Note that the module hostname cannot begin or end with a hyphen (-).
The hostname identifies the IP communicator (onboard or SDI2 module) on the network.
Leave this parameter blank to use the factory default hostname.

Notice!
Leave this parameter blank to use factory default hostname
The factory default hostname begins with the letter B, followed by the last six digits of the modules MAC address.
Use RPS diagnostics or installer (keypad) diagnostics to view the hostname.

Use the hostname on a local network using DHCP. To use the hostname externally, you must enter the hostname in the DNS server.
You can use the hostname to connect to the control panel with RPS or RSC (Remote Security Control), or for module web configuration and diagnostics.
RPS Menu Location
Panel Wide Parameters > Onboard Ethernet Communicator > Module Hostname

4.2.12 TCP/UDP Port Number

Default: 7700
Selections: 0 - 65535
For IP communications with RPS, automation, or Remote Security Control (RSC) in typical installations, keep the TCP/UDP Port at the default

Notice!
Limit unwanted traffic, choose a port number greater than 1023
If you choose to change the port number from the default, select a port number above 1023 to decrease unwanted network traffic.

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

4.2.13 TCP Keep Alive Time

Default: 4 minutes
Selections: Off - 8 Hours
Time between TCP keep-alive messages can be set in either minutes or hours. Keep alive messages make sure that a connection stays active.
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > TCP Keep Alive Time

4.2.14 IPv4 Test Address

Default: 8.8.8.8
Selections: IPv4 address or Domain Name
The control panel pings the IPv4 Test Address to make sure the network configuration settings are correct and that the network is operating.
The default test address works for most networks.

Further information
IP Address and Domain Name formats, page 275
RPS Menu Locations
Panel Wide Parameters > Onboard Ethernet Communicator > IPv4 Test Address

4.2.15 IPv6 Test Address

Default: 2001:4860:4860::8888

Selections: IPv6 address or Domain Name

The control panel pings the IPv6 Test Address to make sure the network configuration settings are correct and that the network is operating.

The default test address works for most networks.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location

Panel Wide Parameters > Onboard Ethernet Communicator > IPv6 Test Address.

4.2.16 Alternate IPv4 DNS server IP address

Default: 0.0.0.0

Selections: 0.0.0.0 to 255.255.255.255

If the IP communicator fails to get an address from the primary server, it tries the alternate DNS server. Enter the IP address for the alternate IPv4 DNS server.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Locations

Panel Wide Parameters > Onboard Ethernet Communicator > Alternate IPv4 DNS server IP address

4.2.17 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

If the IP communicator fails to get an address from the primary server, it tries the alternate DNS server. Enter the IP address for the alternate IPv6 DNS server.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Locations

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

4.3 Cellular Plug-in Module

4.3.1 Inbound SMS

Default: Yes

Selections:

- Enabled (Yes) - you can use inbound SMS text messages to configure the module.
- Disabled (No) - the module does not process inbound SMS text messages.

Notice!

Important configuration information for cellular communication

Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Inbound SMSB450 Cellular > Inbound SMS

4.3.2 Session Keep Alive Period (minutes)

Default: 0
Selections: 0 (disabled) to 1000 (minutes)
Time in minutes between keep-alive messages. Keep alive messages make sure that a connection stays active.
Only change from default for high security UL1610 commercial listed installations.

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Session Keep Alive PeriodKeep Alive Period

4.3.3 Inactivity Timeout (minutes)

Default: 0
Selections: 0 (disable) to 1000 (minutes)
– 0 (disabled) - panel does not monitor for data traffic.
– 1 to 1000 - the time with no data traffic before the control panel ends a session.
Only change from default for high security UL 1610 commercial listed installations requiring low signal notification.

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Inactivity Timeout

4.3.4 Reporting Delay for Low Signal Strength (sec.)

Default: 0 (disabled)
Selections: 0 (disabled), 1 - 3600 (seconds)
Time of low signal strength (red LED on cellular communicator) before the control panel makes a Cellular Low Signal event.
The control panel makes a Cellular Low Signal Restoral event when the signal strength is good (green LED on cellular communicator) for the time you enter at this Reporting Delay for Low Signal Strength parameter.

Notice!
UL Requirement
To meet UL requirements, the entry for this parameter should not exceed 200 seconds.

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for Low Signal Strength

4.3.5 Reporting Delay for No Towers (sec.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0
Selections: 0 (disabled) - 3600 (seconds)
When the cellular plug-in module senses no towers for the seconds set by this parameter, the control panel records a No Towers event and a No IP Address event.
The control panel records a No Tower restoral event when the cellular plug-in module senses one or more towers for the seconds set by this parameter.
The control panel records a No IP Address restoral event when the cellular plug-in module registers with one or more towers and receives an IP address within 60 seconds.

Notice!
When one or more towers are available, 60 second delay for No IP Address event
If the cellular plug-in module successfully registers with one or more towers, but does not receive an IP address within 60 seconds, the control panel creates a No IP Address event.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Reporting Delay for No Towers

4.3.6 Outgoing SMS Length

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 160
Selections: 0 (disabled) to 3600 (characters)
Cellular providers set the limit for SMS message length to 160 characters (the default). The providers reject SMS messages above the limit.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Outgoing SMS Length

4.3.7 IPv4 DNS Server IP Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255

A Domain Name Server (DNS) uses internet domain names or hostnames to supply corresponding IP addresses. In DHCP mode, the DHCP server's default DNS is used. To use a custom DNS server in DHCP mode, enter the custom DNS server's IP address here.

RPS Menu Location

Panel Wide Parameters > Cellular Plug-In Modules > IPv4 DNS server IP address

4.3.8 Alternate IPv4 DNS server IP address

Default: 0.0.0.0

Selections: 0.0.0.0 to 255.255.255.255

Enter the IP address for the alternate IPv4 DNS server.

If the Cellular Plug-in Module fails to get an address from the primary server, the alternate IPv4 server that is specified in this parameter will be used.

RPS Menu Location

Panel Wide Parameters > Cellular Plug-In Modules > Alternate IPv4 DNS server IP address

4.3.9 IPv4 Test Address

Default: 8.8.8.8

Selections: IPv4 address or Domain Name

The control panel pings the IPv4 Test Address to make sure the network configuration settings are correct and that the network is operating.

The default test address works for most networks.

RPS Menu Location

Panel Wide Parameters > Cellular Plug-In Modules > IPv4 Test Address

4.3.10 Network Access Point Name (APN)

Notice!

Important configuration information for cellular communication

Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: eaaa.bssd.vzwentp

Selections: 0-9, A-Z, a-z, **-** , **:** , **.** (up to 60 characters)

To change the access point name (APN) from the default, enter up to 60 characters. The field is case sensitive.

Control panel firmware version 3.07 or later

With control panel firmware version 3.07 or later, when the APN parameter is blank the control panel uses an internal list of Network Access Point Name (APN) values.

When a B442, B443 or B444 plug-in cellular communicator is plugged in, the internal list includes:

- lotst.aer.net
- gne
- wyless.apn (valid only for versions earlier than RPS 6.07)
- wyless.com.attz
- bosch.vzwentp

When a B444-V plug-in cellular communicator is plugged in, the internal list includes:

- bssd.vzwentp

When a B444-A plug-in cellular communicator is plugged in, the internal list includes:

- bssd.attentp

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Name

4.3.11 Network Access Point User Name

Default: Blank
Selections: ASCII characters (up to 30)
Enter up to 30 ASCII characters for the Network Access Point user name.
The user name is case sensitive.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point User Name

4.3.12 Network Access Point Password

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Blank
Selections: ASCII characters (up to 30 characters)
Enter up to 30 ASCII characters for the Network Access Point password.
The password is case sensitive.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > Network Access Point Password

4.3.13 SIM PIN

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Blank
Selections: 0-9 (minimum 4 digits, maximum 8 digits)
Use this parameter only when a PIN is necessary for ICCID cards.
If a SIM PIN is not necessary, leave the field blank.
The SIM PIN shows as asterisks (********) as you enter it. If you enter an invalid SIM PIN, an event is recorded. A report is sent only if the report function is set.

RPS Menu Location
Panel Wide Parameters > Cellular Plug-in Module > SIM PIN

4.4 Cloud Remote Connect

4.4.1 Cloud Remote Connect (Ethernet)

Default: Enabled
Selections: Enabled, Disabled
Use this parameter to enable the Bosch Cloud-based Service, Remote Connect, for communication via an Ethernet connection.

Notice!
Bosch Installer Services, Remote Connect subscription required
Before you can utilize Remote Connect for RPS or RSC connections you need to contact your regional Bosch technical support to set up or get your Account Details.

RPS Menu Location
Panel Wide Parameters > Cloud Remote Connect > Cloud Remote Connect via Ethernet

4.4.2 Cloud Remote Connect (Cellular)

Default: Disabled
Selections: Enabled, Disabled
Use this parameter to enable the Bosch Cloud-based Service, Remote Connect, for communication via a cellular connection.

Notice!
Bosch Installer Services, Remote Connect subscription required
Before you can utilize Remote Connect for RPS or RSC connections you need to contact your regional Bosch technical support to set up or get your Account Details.

RPS Menu Location
Panel Wide Parameters > Cloud Remote Connect > Cloud Remote Connect via Cellular

4.5 IP cameras

The B6512 supports Cameras 1 to 6.
Bosch IP Cameras are integrated into control panel systems by configuring IP connection details in addition to aligning any specific panel points and panel outputs with each IP Camera.
RPS operators have the ability to import IP Camera connection details using an export file created from the Bosch Configuration Manager application.

4.5.1 Camera name (first language)

Default: Camera #
Selections: 0-32 characters (Latin-1 8-bit (ISO/IEC 8859-1) character set)
Enter a name for a Bosch IP camera in the control panel's first language.
Set first and second languages in the Panel Data - View window. Refer to Panel Data - View > Panel Info tab > Additional Info.
Language options are: English, Spanish, French and Portuguese.

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

4.5.2 Camera name (second language)

Default: Blank
Selections: 0-32 characters (Latin-1 8-bit (ISO/IEC 8859-1) character set)
Enter a name for a Bosch IP camera in the control panel's second language.
Set first and second languages in the Panel Data - View window. Refer to Panel Data - View > Panel Info tab > Additional Info.
Language options are: English, Spanish, French and Portuguese.

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

4.5.3 URL or IP address

Default: Blank

Selections: 0-128 ASCII characters

This parameter sets the URL or IP address for the Bosch IP camera.

The control panel or RSC application uses the camera's URL or IP address to communicate with the camera over a network.

RPS Menu Location

Panel Wide Parameters > IP Cameras > URL or IP Address

4.5.4 Camera Inputs-Outputs

Using this option, RPS operators can interact with a consolidated view of Bosch IP Camera Integrations, including panel point assignments and panel output assignments. The window provides a visual map to assist the review and the assignment of panel points and panel outputs available for each individual IP camera.

Control panels act on Bosch IP Camera Video Analytics by registering and receiving information from the IP Camera Task Alarms (1-8) and Wired Inputs (1, 2).

Control panels initiate Bosch IP Cameras to operate by using the IP Camera Alarms (1-4).

Use the window to:

- view and assign the available points for the IP camera. Current point source shows the current programming for each point available for use with the specific IP camera. Assign to IP Camera assigns the point source of the corresponding panel point(s). This is the identical programming set using Points>Point Assignment>Point Source>IP Camera.
- view and assign the available output source for the IP camera. Current output source shows the current programming for each output available for use with the specific IP Camera. Assign to IP Camera assigns the output source to IP camera for the corresponding panel output(s). This is the identical programming set using Outputs>Output Assignments>Output Source>IP Camera.

For example, a camera (Camera 1) configured on physical points 10-19, can use Output 11-14. Another camera (Camera 32) configured on Point 320-329, can use Output 321-324.

- **Open Bosch IP Camera URL** - select this button for RPS to use the IP camera connection details and open a desktop browser to the individual camera web page.
- **Open Bosch Configuration Manager** - select this button for RPS to open the Bosch Configuration Manager desktop application.

To assign points and outputs to an IP camera automatically:

1. Select a camera to configure and select the Camera Inputs-Outputs parameter.
2. Double-click **Tasks/Alarms**.
3. In the Camera to Panel Communication table, select Assign to IP Camera to assign an available point to the camera.
4. In the Panel to Camera Communication table, select an available output source for the camera.
5. Click **OK**.

Access the point assignments and output assignments to view the assignment results.

RPS Menu Location

Panel Wide Parameters > IP Cameras > Camera Inputs-Outputs

4.6 Bosch Connected Cameras

Products

– B6512 with on-board IP communicator
– All Bosch IP cameras

Implementation

After establishing that each IP camera is available for network operations, configure control panels to integrate Bosch IP cameras as panel inputs, outputs, or both.

Environment

Install compatible 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 parameters configure network communication and supervision with connected Bosch IP cameras.

Other panel configuration for integrating Bosch IP cameras

Point Source parameter "IP Camera" (*Source, page 183*)
Output Source parameter "IP Camera" (*Output Source, page 143*)

4.6.1 RCP+ port

Default: 1756
Selections: 0-65535
This parameter sets the port number a Bosch IP camera monitors for RCP+ protocol. Only change from the default, 1756, if an IP camera is configured to monitor a different port.

RPS Menu Location

Panel Wide Parameters > IP Cameras > Bosch Connected Camera > RCP+ Port #

4.6.2 Service password

Default: Blank
Selections: Blank(disable), 1-32 characters
Enter the password necessary to access the Bosch IP camera's data.
The password is case sensitive.

RPS Menu Location

Panel Wide Parameters > IP Cameras > Bosch Connected Camera > Service Password

4.6.3 Supervision period

Default: 0: Disabled
Selections: 0: Disabled, 1-10 min (minutes)
The length of time a Bosch IP camera must be missing before the control panel makes a camera missing event.

RPS Menu Location

Panel Wide Parameters > IP Cameras > Bosch Connected Camera > Supervision Period

4.7 Live (video)

Products

– B6512 with on-board IP communicator
– All Bosch IP cameras
– RSC (Remote Security Control) mobile app

– BSM (Bosch Security Manager) mobile app

Applications
Live video allows end users to see video of associated IP cameras when logged in and authorized using Bosch mobile apps.

Implementation
Live video can be configured for Bosch or other IP Cameras that support live video image access through HTTP or HTTPS authenticated access. While networking each IP camera, make sure that the network setting details to allow basic authentication when using HTTP are enabled (on).

Panel Configuration
The RSC and Bosch Mobile apps will use the Port #, Use HTTPS?, User Name, and Password to access video images within the IP cameras.

Notice!
HTTP and basic authentication
RPS Live View user and password may not operate unless the camera is configured (not RPS configuration) to allow basic authentication for HTTP connections. Once enabled, the RPS configured Live View user and password will be used by Bosch mobile apps to securely access video.

RPS programming for IP cameras
The recommendation configuration enables Bosch Mobile app users to view IP camera Live (video) securely:
– URL or IP Address: <match the actual IP camera settings>
– Live (Video) > Port #: <match the IP camera settings>
– Each IP camera with a unique port (e.g. Camera 2; Port# 10042, Camera 3; Port# 10043)
– Live (Video) Use HTTPs?: Yes
– Live (Video) User Name: <match the IP camera settings>
– Live (Video) Password: <match IP camera settings>

4.7.1 Port

Default: 80
Selections: 0-65535
Enter the port number the RSC (Remote Security Control) application uses for IP communications and live video with the camera.
When the live viewer URL is assigned to a router, configure the router with the port number you enter here.
When using HTTPS, set this port number to 443.
The B6512 supports Cameras 1 to 6.

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

4.7.2 Use HTTPS?

Default: No
Selections:
Yes - Enable HTTPS (encrypts data for secure Bosch IP camera to RSC communications).

No - Disable HTTPS
Set to Yes if the live viewer requires HTTPS.
When HTTPS is set to Yes, set Panel Wide Parameters > IP Cameras > Live (Video) > Port # to 443
The B6512 supports Cameras 1 to 6.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > Use HTTPS?

4.7.3 User Name

Default: live
Selections: A-Z, a-z, 0-9, up to 32 characters.
Enter the User Name as it is entered in the camera. The RSC application uses the User Name and Password to show video from the camera.
The B6512 supports Cameras 1 to 6.

RPS Menu Location
Panel Wide Parameters > IP Cameras > Live (Video) > User Name

4.7.4 Password

Default: Blank
Selections: A-Z, a-z, 0-9, up to 32 characters.
Enter the Password as it is entered in the camera. The RSC application uses the User Name and Password to show video from the camera.
The B6512 supports Cameras 1 to 6.

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

4.8 Reporting Overview

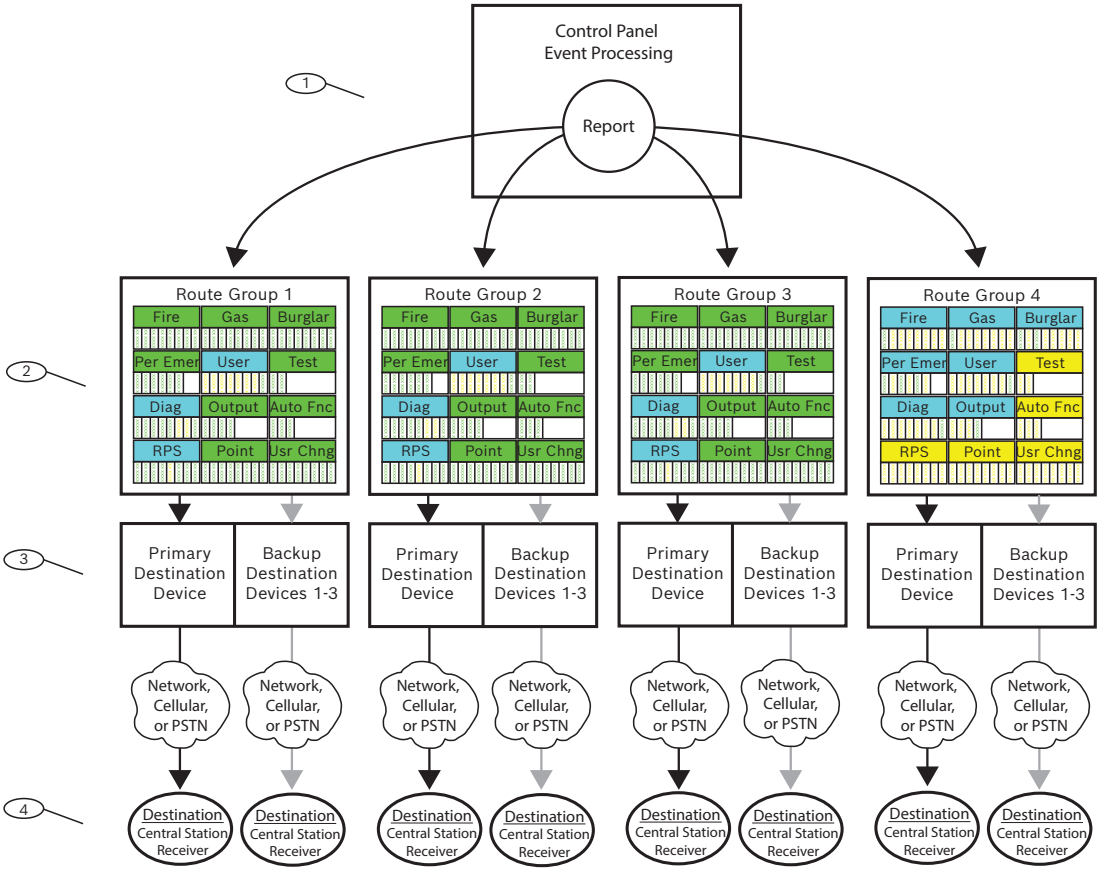


Figure 4.1:

1 - Reports begin with events

The control panel monitors points, modules, keypads, and panel power (AC and battery) for off-normal conditions. When the panel detects an off-normal condition (or a restoral from an off-normal condition), the panel generates an event. The control panel adds events to the history log and can send events as reports to a central station receiver or to users as Personal Notifications.

When the control panel has reports to send, the panel sorts the reports into the Route Groups (1 to 4). Each Route Group has its own communicator, with a Primary Destination Device, and up to 3 Backup Destination Devices (backup destinations), to send the reports in the Route Group to a central station receiver.

2 - Report Routing parameters

Use the *Report Routing, page 50* parameters to configure the four Route Groups (1 to 4). The parameters below the Report Routing heading assign reports to Route Groups by category (all Fire Reports or all Burglar Reports for example) or individually (Fire Alarm for example).

You can assign reports to one or more Route Groups.

3 - Communicator parameters

The parameters below the *Communicator, overview, page 63* heading assign a Primary Destination Device and up to 3 Backup Destination Devices to each Route Group. The control panel uses the Route Group's Primary Destination Device first to send reports. If the

Primary Destination Device fails to send the report, the control panel makes a Comm Trouble Event and changes to the First Backup Destination Device, and if configured, the Second Backup Destination Device, and finally the Third Backup Destination Device.
The control panel makes up to ten communication attempts, changing between the Primary and Backup Destination Devices, to send reports from a Route Group based on a set of retry combinations shown in the table in the *Communicator, overview, page 63* help topic. If unsuccessful after the 10 attempts, it makes a Comm Fail Event.

4 - Destinations

The control panel sends reports from each Route Group using their Primary and Backup Destination Devices to the destinations configured for the device.
Configure for Onboard IP Destinations here: *On Board Ethernet (IP) Communicator, page 34*, and here: *Enhanced Communication, page 68*.
Configure for Plug -in Cellular IP Destinations here: *Cellular Plug-in Module, page 38*, and here *Enhanced Communication, page 68*. Refer to *Configuring for Cellular Service, page 272* for more information.
Configure for Plug-in Phone Destinations here: *Phone and Phone Parameters, page 31*.
Configure for SDI2 Address Destinations here: *(B42x) IP Communicator, page 256* or here: *B450 cellular, page 261*, and here: *Enhanced Communication, page 68*.

Route Group priority

Route Group 1 has the highest priority. Route Group 4 has the lowest priority. When there are reports in more than one Report Group to be sent at the same time, the control panel sends the report in the highest priority Route Group first. For example if there are reports in Route Group 2 and Route Group 3, the control panel sends the report in Route Group 2 first.

Priority within a Route Group

Within a Route Group, reports to be sent are prioritized as shown. The control panel sends the highest priority report first. 1 is the highest priority.

1. **Diagnostic Reports**: Watchdog Reset, Reboot.
   RPS Reports: Remote Reset.
2. **Fire Reports**: Fire Alarm.
3. **Gas Reports**: Gas Alarm.
4. **Personal Emergency Reports**: Medical Alarm, Silent / Hold-up Alarm, Panic Alarm, Duress.
5. **Burglar Reports**: Alarm Report.
6. **Fire Reports**: Fire Cancel.
   Gas Reports: Gas Cancel.
   Burglar Reports: Non-Fire Cancel.
   Diagnostic Reports: SDI2 Device Failure, Parameter Checksum Fail, Phone Line Fail, AC Failure, Battery Missing, Battery Low, Battery Restoral, Route Comm Fail, Route Comm Fail Restore.
7. **Fire Reports**: Fire Restoral (after Alarm), Fire Missing, Fire Trouble, Fire Supervision, Fire Restoral (after Trouble), Fire Supervision Missing, Fire Supervision Restoral.
   Gas Reports: Gas Restoral from Alarm, Gas Missing, Gas Trouble, Gas Supervision, Gas Restoral from Trouble, Gas Supervision Missing, Gas Supervision.
   Burglar Reports: Non-Fire Supervision.
   Personal Emergency Reports: Medical Alarm Restoral, Silent / Hold-up Alarm Restoral, Panic Alarm Restoral.

8. **Burglar Reports**: Burg Restore (after Trouble), Missing Alarm, Trouble Report, Missing Trouble, Point Bus Fail, Point Bus Restoral, Alarm Restore, Supervision Missing, Unverified Event.
9. **User Reports**: Forced Point, Was Force Armed, Forced Close, Forced Close Part On Instant, Forced Close Part On Delay.
   Diagnostic Reports: Service Smoke Detector, Service Smoke Detector Restore.
   Output Reports: Sensor Reset, Output Set, Output Reset.
   Auto Function Reports: Sked Executed, Sked Changed, Fail to Execute (Sked).
   Point Reports: Bypass, Bypass Restore.
   User Change Reports: Change Level.
10. **Burglar Reports**: User Code Tamper.
    User Reports: Fail to Open, Fail to Close, Extend Close Time, Opening Report, Closing Report, Point Opening, Point Closing, Part On Instant, Part On Delay.
    Test Reports: Status Report, Test Report.
    Diagnostic Reports: SDI2 Device Restoral, Phone Line Restoral, AC Restoral, Checksum Fail, Network Fail (and Restoral), Network Condition, RF Interference (and Restore), Equipment Fail (and Restore), Personal Notification Communication Trouble (and Restore).
    RPS Reports: Event Log Threshold, Event Log Overflow, Parameters Changed, RPS Access OK, RPS Access Fail, Remote Reset, Program Access OK, Program Access Fail.
    Point Reports: Service Start, Service End, Fire Walk Start, Fire Walk End, Walk Test Start, Walk Test End, Extra Point, RF Low Battery, RF Battery Restore.
    User Change Reports: Date Changed, Time Changed, Delete User, User Code Change, Area Watch, Keyfob Assigned, Keyfob Removed, Change Level.
    Access Reports: Access Granted, No Entry, Door Left Open, Cycle Door, Door Unlocked, Door Secure, Door Request, Door Locked.

4.9 Report Routing

Default:

Report Category	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Fire Reports, page 51	Yes	Yes	Yes	Custom
Gas Reports, page 51	Yes	Yes	Yes	Custom
Burglar Reports, page 52	Yes	Yes	Yes	Custom
Personal Emergency Reports, page 52	Yes	Yes	Yes	Custom
User Reports, page 52	Custom	Custom	Custom	Custom
Test Reports, page 53	Yes	Yes	Yes	No
Diagnostic Reports, page 53	Custom	Custom	Custom	Custom
Output Reports, page 53	Yes	Yes	Yes	Custom
Auto Function Reports, page 53	Yes	Yes	Yes	No
RPS Reports, page 54	Custom	Custom	Custom	No

Report Category	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Point Reports, page 54	Yes	Yes	Yes	No
User Change Reports, page 54	Yes	Yes	Yes	No
Access Reports, page 54	Yes	Yes	Yes	Yes
Environmental Reports, page 63	Yes	Yes	Yes	Custom

Selections:

– Yes - assign all of the reports in this category to the Route Group.
– No - do not assign any of the reports in this category to the Route Group.

Custom - you can not select Custom. Custom shows for a category when at least one of the reports in the category is configured individually.

Notice!

Configuration for individual reports lost on change from Custom to Yes or No

When Custom appears for a category of reports, it indicates that not all of the reports are set the same (all Yes or all No). The reports have been set individually.

If you change the reports for a category from Custom to Yes or No, the configuration for the individual reports in the category is lost. To individually re-assign reports from a report category to a Route Group, you must click on the report category in the menu tree, *Fire Reports, page 55* for example.

RPS Menu Location

Panel Wide Parameters > Report Routing

Fire Reports

Reports in the Fire category:

– Fire Alarm
– Fire Restoral (After Alarm)
– Fire Missing
– Fire Trouble
– Fire Supervision
– Fire Restoral (After Trouble)
– Fire Cancel
– Fire Supervision Missing
– Fire Supervision Restoral

To individually assign reports from the Fire category to a Route Group, click *Fire Reports, page 55* in the menu tree.

Gas Reports

Reports in the Gas category:

– Gas Alarm
– Gas Restoral From Alarm
– Gas Missing.
– Gas Trouble
– Gas Supervision
– Gas Restoral From Trouble
– Gas Cancel

– Gas Supervision Missing
– Gas Supervision Restoral

To individually assign reports from the Gas category to a Route Group, click *Gas Reports, page 56* in the menu tree.

Burglar Reports

Reports in the Burglar category:

– Alarm Report
– Burg Restore (After Trouble)
– Duress
– Missing Alarm
– User Code Tamper
– Trouble Report
– Missing Trouble
– Non-Fire Supervision
– Point Bus Fail
– Point Bus Restoral
– Non-Fire Cancel
– Alarm Restore
– Supervision Missing
– Unverified Event

To individually assign reports from the Burglar category to a Route Group, click *Burglar Reports, page 56* in the menu tree.

Personal Emergency Reports

Reports in the Personal Emergency category:

– Medical Alarm
– Medical Alarm Restoral (reserved for future use)
– Silent / Hold-Up Alarm
– Silent / Hold-Up Alarm Restoral
– Panic Alarm
– Panic Alarm Restoral (reserved for future use)

To individually assign reports from the Personal Emergency category to a Route Group, click *Personal Emergency Reports, page 57* in the menu tree.

User Reports

Reports in the User category:

– 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
– Closing Report
– Forced Close Part On Instant
– Forced Close Part On Delay
– Part On Instant
– Part On Delay

To individually assign reports from the User category to a Route Group, click *User Reports, page 57* in the menu tree.

Test Reports

Reports in the Test category:

– Status Report
– Test Report

To individually assign reports from the Test category to a Route Group, click *Test Reports, page 58* in the menu tree.

Diagnostic Reports

Reports in the Diagnostic category:

– SDI2 Device Failure
– SDI2 Device Restoral
– Watchdog Reset
– Parameter Checksum Fail
– Reboot
– Phone Line Fail
– Phone Line Restoral
– AC Failure
– AC Restoral
– Battery Missing
– Battery Low
– Battery Restoral
– Route Comm Fail
– Route Comm Restore
– Checksum Fail
– Network Fail
– Network Restoral
– Network Condition
– RF Interference
– RF Interference Restoral
– Equipment Fail
– Equipment Fail Restoral
– Service Smoke Detector
– Service Smoke Detector Restoral
– Personal Notification Communication Trouble
– Personal Notification Communication Trouble Restoral

To individually assign reports from the Diagnostic category to a Route Group, click *Diagnostic Reports, page 59* in the menu tree.

Output Reports

Reports in the Output category:

– Sensor Reset
– Output Set
– Output Reset

To individually assign reports from the Output category to a Route Group, click *Output Reports, page 60* in the menu tree.

Auto Function Reports

Reports in the Auto Function category:

– Sked Executed

– Sked Changed
– Fail to Execute

To individually assign reports from the Auto Function category to a Route Group, click *Auto Function Reports, page 60* in the menu tree.

RPS Reports

Reports in the RPS category:
– Event Log Threshold
– Event Log Overflow
– Parameters Changed
– RPS Access OK
– RPS Access Fail
– Remote Reset
– Program Access OK
– Program Access Fail

To individually assign reports from the RPS category to a Route Group, click *RPS Reports, page 60* in the menu tree.

Point Reports

Reports in the Point category:
– Service Start
– Service End
– Fire Walk Start
– Fire Walk End
– Walk Test Start
– Walk Test End
– Extra Point
– Send Point Text
– RF Low Battery
– RF Low Battery Restore
– Bypass
– Bypass Restore

To individually assign reports from the Point category to a Route Group, click *Point Reports, page 61* in the menu tree.

User Change Reports

Reports in the User Change category:
– Date Changed
– Time Changed
– Delete User
– User Code Change
– Area Watch
– Keyfob Assigned
– Keyfob Removed
– Change Level

To individually assign reports from the User Change category to a Route Group, click *User Change Reports, page 62* in the menu tree.

Access Reports

Reports in the Access category:
– Access Granted
– No Entry

- Door Left Open
- Cycle Door
- Door Unlocked
- Door Secure
- Door Request
- Door Locked

To individually assign reports from the Access category to a Route Group, click *Access Reports, page 62* in the menu tree.

Notice!
UL 985 requirement for Household Fire Warning System Units
When configuring transmission defaults, make sure that communication tests are done monthly or earlier, and that communication failure annunciation (total delay created by heartbeat settings and retry counts) is not more than 7 days.

Environmental Reports
Reports in the Environmental category:
- Water Alarm
- Water Restoral
- High Temp Alarm
- High Temp Restoral
- Low Temp Alarm
- Low Temp Restoral

To individually assign reports from the Environmental category to a Route Group, click *Environmental Reports, page 63* in the menu tree.

4.9.1 Fire Reports

Default:

Fire Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Fire Alarm	Yes	Yes	Yes	Yes
Fire Restoral (after Alarm)	Yes	Yes	Yes	No
Fire Missing	Yes	Yes	Yes	No
Fire Trouble	Yes	Yes	Yes	No
Fire Supervision	Yes	Yes	Yes	No
Fire Restoral (after Trouble)	Yes	Yes	Yes	No
Fire Cancel	Yes	Yes	Yes	No
Fire Supervision Missing	Yes	Yes	Yes	No
Fire Supervision Restoral	Yes	Yes	Yes	No

Selections:
- Yes - assign this report to the Route Group.
- No - do not assign this report to the Route Group.

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

4.9.2 Gas Reports

Default:

Gas Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Gas Alarm	Yes	Yes	Yes	Yes
Gas Restoral from Alarm	Yes	Yes	Yes	No
Gas Missing	Yes	Yes	Yes	No
Gas Trouble	Yes	Yes	Yes	No
Gas Supervision	Yes	Yes	Yes	No
Gas Restoral from Trouble	Yes	Yes	Yes	No
Gas Cancel	Yes	Yes	Yes	No
Gas Supervision Missing	Yes	Yes	Yes	No
Gas Supervision Restoral	Yes	Yes	Yes	No

Selections:
– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

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

4.9.3 Burglar Reports

Default:

Burglar Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Alarm Report	Yes	Yes	Yes	Yes
Burg Restore (after Alarm)	Yes	Yes	Yes	No
Duress	Yes	Yes	Yes	Yes
Missing Alarm	Yes	Yes	Yes	No
User Code Tamper *	Yes	Yes	Yes	No
Trouble Report	Yes	Yes	Yes	No
Missing Trouble	Yes	Yes	Yes	No
Non-Fire Supervision	Yes	Yes	Yes	No
Point Bus Fail	Yes	Yes	Yes	No
Point Bus Restoral	Yes	Yes	Yes	No
Non-Fire Cancel	Yes	Yes	Yes	No

Burglar Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Alarm Restore	Yes	Yes	Yes	No
Supervision Missing	Yes	Yes	Yes	No
Unverified Event	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.

– No - do not assign this report to the Route Group.

***** A panel sends a User Code Tamper event when a user consecutively enters an invalid passcode 7 times at the keypad.

For Mode 2 connection types, such as RSC or automation, a panel sends a User Code Tamper event when the user consecutively enters 15 invalid passcodes.

RPS Menu Location

Panel Wide Parameters > Report Routing > Burglar Reports.

4.9.4 Personal Emergency Reports

Default:

Personal Emergency Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Medical Alarm	Yes	Yes	Yes	Yes
Medical Alarm Restoral	Yes	Yes	Yes	No
Silent / Hold-Up Alarm	Yes	Yes	Yes	Yes
Silent / Hold-Up Alarm Restoral	Yes	Yes	Yes	No
Panic Alarm	Yes	Yes	Yes	Yes
Panic Alarm Restoral	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.

– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Personal Emergency Reports.

4.9.5 User Reports

Default:

User Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Forced Point	Yes	Yes	Yes	No
Point Opening	Yes	Yes	Yes	No
Point Closing	Yes	Yes	Yes	No

User Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Was Forced Armed	Yes	Yes	Yes	No
Fail to Open	Yes	Yes	Yes	No
Fail to Close	Yes	Yes	Yes	No
Extent Close Time	Yes	Yes	Yes	No
Opening Report	No	No	No	No
Forced Close	No	No	No	No
Closing Report	No	No	No	No
Forced Close Part On Instant	No	No	No	No
Forced Close Part On Delay	No	No	No	No
Part On Instant	No	No	No	No
Part On Delay	No	No	No	No
Send User Text	Yes	Yes	Yes	Yes

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > User Reports.

4.9.6 Test Reports

Default:

Test Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Status Report	Yes	Yes	Yes	No
Test Report	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Test Reports.

4.9.7 Diagnostic Reports

Default:

Diagnostic Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
SDI2 Device Failure	Yes	Yes	Yes	No
SDI2 Device Restoral	Yes	Yes	Yes	No
Watchdog Reset	Yes	Yes	Yes	No
Parameter Checksum Fail	Yes	Yes	Yes	No
Reboot	Yes	Yes	Yes	No
Phone Line Fail	Yes	Yes	Yes	No
Phone Line Fail Restoral	Yes	Yes	Yes	No
AC Failure	Yes	Yes	Yes	No
AC Restoral	Yes	Yes	Yes	No
Battery Missing	Yes	Yes	Yes	No
Battery Low	Yes	Yes	Yes	No
Battery Restoral	Yes	Yes	Yes	No
Route Comm Fail	Yes	Yes	Yes	No
Route Comm Restoral	Yes	Yes	Yes	No
Checksum Fail	Yes	Yes	Yes	No
Network Fail	No	No	No	No
Network Restoral	No	No	No	No
Network Condition	No	No	No	No
RF Interference	Yes	Yes	Yes	No
RF Interference Restore	Yes	Yes	Yes	No
Equipment Fail	Yes	Yes	Yes	No
Equipment Fail Restore	Yes	Yes	Yes	No
Service Smoke Detector	Yes	Yes	Yes	No
Service Smoke Detector Restore	Yes	Yes	Yes	No
Personal Notification Communication Trouble	No	No	No	No
Personal Notification Communication Trouble Restore	No	No	No	No
Send Version Text	Yes	Yes	Yes	Yes

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

Enable Route Comm Fail and Rout Comm Restore reports in only one route group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Diagnostic Reports.

4.9.8 Output Reports

Default:

Output Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Sensor Reset	Yes	Yes	Yes	No
Output Set	Yes	Yes	Yes	No
Output Reset	Yes	Yes	Yes	No
Send Output Name Text	Yes	Yes	Yes	Yes

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Output Reports.

4.9.9 Auto Function Reports

Default:

Auto Function Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Sked Executed	Yes	Yes	Yes	No
Sked Changed	Yes	Yes	Yes	No
Fail to Execute	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Auto Function Reports.

4.9.10 RPS Reports

Default:

RPS Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Event Log Threshold	Yes	Yes	Yes	No
Event Log Overflow	Yes	Yes	Yes	No

RPS Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Parameters Changed	Yes	Yes	Yes	No
RPS Access OK	Yes	Yes	Yes	No
RPS Access Fail	No	No	No	No
Remote Reset	Yes	Yes	Yes	No
Program Access OK	Yes	Yes	Yes	No
Program Access Fail	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > RPS Reports.

4.9.11 Point Reports

Default:

Point Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Service Start	Yes	Yes	Yes	No
Service End	Yes	Yes	Yes	No
Fire Walk Start	Yes	Yes	Yes	No
Fire Walk End	Yes	Yes	Yes	No
Walk Test Start	Yes	Yes	Yes	No
Walk Test End	Yes	Yes	Yes	No
Extra Point	Yes	Yes	Yes	No
Send Point Text	Yes	Yes	Yes	No
RF Low Battery	Yes	Yes	Yes	No
RF Low Battery Restore	Yes	Yes	Yes	No
Bypass	Yes	Yes	Yes	No
Bypass Restore	Yes	Yes	Yes	No
Point Tamper Alarm	Yes	Yes	Yes	Yes
Point Tamper Alarm Restore	Yes	Yes	Yes	Yes

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

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

4.9.12 User Change Reports

Default:

User Change Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Date Changed	Yes	Yes	Yes	Yes
Time Changed	Yes	Yes	Yes	No
Delete User	Yes	Yes	Yes	No
User Code Change	Yes	Yes	Yes	No
Area Watch	Yes	Yes	Yes	No
Keyfob Assigned	Yes	Yes	Yes	No
Keyfob Removed	Yes	Yes	Yes	No
Change Level	Yes	Yes	Yes	Yes

Selections:
– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

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

4.9.13 Access Reports

Default:

Access Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Access Granted	Yes	Yes	Yes	Yes
No Entry	Yes	Yes	Yes	Yes
Door Left Open	Yes	Yes	Yes	Yes
Cycle Door	Yes	Yes	Yes	Yes
Door Unlocked	Yes	Yes	Yes	Yes
Door Secure	Yes	Yes	Yes	Yes
Door Request	Yes	Yes	Yes	Yes
Door Locked	Yes	Yes	Yes	Yes

Selections:
– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

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

4.9.14 Environmental Reports

Default:

Environmental Reports	Route Group 1	Route Group 2	Route Group 3	Route Group 4
Water Alarm	Yes	Yes	Yes	Yes
Water Restoral	Yes	Yes	Yes	No
High Temp Alarm	Yes	Yes	Yes	Yes
High Temp Restoral	Yes	Yes	Yes	No
Low Temp Alarm	Yes	Yes	Yes	Yes
Low Temp Restoral	Yes	Yes	Yes	No

Selections:

– Yes - assign this report to the Route Group.
– No - do not assign this report to the Route Group.

RPS Menu Location

Panel Wide Parameters > Report Routing > Environmental Reports

4.10 Communicator, overview

There are four Route Groups. Reports are assigned to Route Groups by category (Fire Reports or Burglar Reports) or individually (Fire Alarm). Refer to *Reporting Overview, page 48* for information about assigning reports to Route Groups.
Use the parameters to assign a Primary Destination Device and up to 3 Backup Destination Devices to each Route Group.
If the Primary Destination Device fails to send the report, the control panel changes to the first Backup Destination Device and continues through each configured Backup Destination Devices (First, Second, and Third) until the report is successfully sent.

Notice!
B5512, B4512, B3512 V2 panels do not have a Second or Third Backup Destination Device.

The control panel makes up to ten attempts to send reports in a Route Group using the Primary and Backup Destination Devices. The control panel changes between the Primary and Backup Destination Devices as shown in the table. After 10 unsuccessful attempts, the control panel issues a Comm Fail Event.
If no Backup Destination Devices are configured, the control panel uses the Primary Destination Device for all ten attempts.

Configured destinations	Primary and First Backup Destination Devices	Primary, First, and Second Backup Destination Devices	Primary, First, Second, and Third Backup Destination Devices
Send attempt:			

1	Primary Destination Device	Primary Destination Device	Primary Destination Device
2	Primary Destination Device	Primary Destination Device	Primary Destination Device
3	First Backup Destination Device	First Backup Destination Device	First Backup Destination Device
4	First Backup Destination Device	First Backup Destination Device	First Backup Destination Device
5	Primary Destination Device	Second Backup Destination Device	Second Backup Destination Device
6	First Backup Destination Device	Second Backup Destination Device	Second Backup Destination Device
7	Primary Destination Device	Primary Destination Device	Third Backup Destination Device
8	First Backup Destination Device	First Backup Destination Device	Third Backup Destination Device
9	Primary Destination Device	Second Backup Destination Device	Primary Destination Device
10	First Backup Destination Device	Primary Destination Device	First Backup Destination Device

COMM TROUBLE, COMM FAIL events

When the Primary Destination Device fails to connect to the central station receiver after two attempts, the control panel switches to the Backup Destination Device. The control panel sends the original report along with a COMM TROUBLE report. If no Backup Destination Devices are configured, a COMM TROUBLE report is sent.

The control panel sends a COMM RESTORE event when it successfully sends a report using the Primary Destination Device.

If the Primary Destination Device is an IP Destination (Onboard IP, Plug-in Cellular IP, SDI2 Address 1, or SDI2 Address 2), the control panel sends the original event along with a COMM TROUBLE report that includes an SDI2 number modifier (SDI2##). The SDI2 modifier identifies the IP Destination Device type as shown in the tables:

IP Destination Type	SDI2 number modifier for IP Destination 1	SDI2 number modifier for IP Destination 2	SDI2 number modifier for IP Destination 3	SDI2 number modifier for IP Destination 4
Onboard Ethernet	10	20	30	40
Plug-in Cellular	18	28*	38	48
SDI2 Address 1	11	21	31	41

*For example, a COMM TROUBLE report for Route Group 1 with the Primary Destination Device assigned to Plug-in or Onboard Cellular, Destination 2 will be named - COMM TROUBLE RG1 SDI228.

The control panel makes COMM TROUBLE events when positive acknowledgement from the central station receiver to polls are not received after the configured number of retries. If all attempts to both the Primary Destination Device and the Backup Destination Devices fail, the control panel makes a COMM FAIL RG# event. The control panel does not make COMM RESTORE events for COMM FAIL events.

Notice!
CAN/ULC S304 requirement, do not clear pending reports
When CAN/ULC S304 is set to YES, the control panel does not clear pending reports before creating a COMM FAIL event. It continues to queue reports for the failed route until one of the failed routes in the route group restores. If the queue reaches the capacity of the panel event log, the oldest reports are cleared (overwritten).

Notice!
UL 985 requirement for Household Fire Warning System Units
When configuring transmission defaults, make sure that communication tests are done monthly or earlier, and that communication failure annunciation (total delay created by heartbeat settings and retry counts) is not more than 7 days.

4.10.1 Primary Destination Device

Default: No Device

Selections:
- No Device
- Onboard IP Destination 1
- Onboard IP Destination 2
- Onboard IP Destination 3
- Onboard IP Destination 4
- (Plug-in) Cellular Destination 1
- (Plug-in) Cellular Destination 2
- (Plug-in) Cellular Destination 3
- (Plug-in) Cellular Destination 4
- (Plug-in) Phone Destination 1
- (Plug-in) Phone Destination 2
- (Plug-in) Phone Destination 3
- (Plug-in) Phone Destination 4
- SDI2 address 1 Destination 1
- SDI2 address 1 Destination 2
- SDI2 address 1 Destination 3
- SDI2 address 1 Destination 4

Select the Primary Destination Device for Route Groups. The control panel uses the device to send reports to the central station receiver.
The Primary Destination Device selection assigns a communicator (onboard IP communicator, plug-in cellular communicator, plug-in phone communicator, or SDI2 module) to a destination (*Network Address, page 69*, or *Phone and Phone Parameters, page 31*)

Further information
For more information on how the control panel sends reports, refer to *Reporting Overview, page 48* and *Communicator, overview, page 63*.

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

4.10.2 Backup Destination Devices

Default: No Device
Selections:
- No Device
- Onboard IP Destination 1
- Onboard IP Destination 2
- Onboard IP Destination 3
- Onboard IP Destination 4
- (Plug-in) Cellular Destination 1
- (Plug-in) Cellular Destination 2
- (Plug-in) Cellular Destination 3
- (Plug-in) Cellular Destination 4
- (Plug-in) Phone Destination 1
- (Plug-in) Phone Destination 2
- (Plug-in) Phone Destination 3
- (Plug-in) Phone Destination 4
- SDI2 address 1 Destination 1
- SDI2 address 1 Destination 2
- SDI2 address 1 Destination 3
- SDI2 address 1 Destination 4

Select up to 3 Backup Destination Devices (First, Second, Third) for a Route Group. The control panel uses the backup device to send reports to the central station receiver when the primary device fails.
The Backup Destination Device selections assigns a communicator (onboard IP communicator, plug-in cellular communicator, plug-in phone communicator, or SDI2 module) to a destination (*Network Address, page 69*, or *Phone and Phone Parameters, page 31*).
Do not select the same destination device for both the Primary Destination Device and Backup Destination Device for a Route Group.

Further information
For more information on how the control panel sends reports, refer to *Reporting Overview, page 48* and *Communicator, overview, page 63*.

RPS Menu Location
Panel Wide Parameters > Communicator > Backup Destination Device

4.10.3 RG Same Network Receiver

Default: Yes
Selections:
- Yes - the control panel uses the same authentication key for the primary and backup destinations.
- No - the control panel uses separate authentication keys for the primary and backup destinations.

Set this parameter to Yes when:
- The Primary Destination Device and the Backup Destination Devices are set to IP devices (onboard, cellular, or SDI2) and Destinations configured in Enhanced Communication.

– The Destinations are configured for the same central station receiver, but with different IP Addresses that can be accessed from different networks (LAN/WAN and the internet for example).

When this parameter is set to Yes and the primary destination and the backup destination use different poll rates, and the control panel detects a communication trouble on the primary or backup destination device, the working destination device immediately changes to the faster poll rate.

When this parameter is set to No and the control panel detects a communication trouble on the primary or backup destination device, the working destination device continues to use the configured poll rate.

This parameter is typically set to No when one of the destination devices is set to an Onboard IP or SDI2 device, and the other to a Plug-in Cellular IP device. Poll Rate for cellular destinations is typically set to a slower rate (4 hours).

Poll rates of 5 minutes or faster could exceed your cellular data plan. Attend to any Communication Trouble events as soon as possible.

RPS Menu Location

Panel Wide Parameters > Communicator > RG Same Network Receiver

4.10.4 Time Synchronization

Default:

Route Group 1: Yes

Route Groups 2-4: No

Selections:

– Yes - synchronize control panel time and date with the central station receiver.

– No - do not synchronize control panel time and date with the central station receiver.

Notice!

Time Synchronization set to Yes

When Time Synchronization is set to **Yes**, you must set the Primary Destination Device or Backup Destination Devices to **Onboard IP**, **Plug-in Cellular IP** or **SDI2** and also set the Reporting Format for the Destination to **Modem4**.

Time Synchronization is available for all route groups, but can only be set to Yes for one route group at a time.

Control panel time off by 30 minutes or Less

When the control panel time is off by 30 minutes or less and the control panel's time is behind the correct time, the control panel counts seconds faster than one per second. If the control panel's time is forward of the correct time, the control panel counts seconds slower than one per second.

The control panel counts seconds in this mode until the control panel time synchronizes with the central station receiver. Every second occurs and no seconds are repeated. Therefore no Skeds, scheduled events, or window starts and stops are skipped or repeated.

Control panel time off by more than 30 minutes

When the control panel time is off by more than 30 minutes, the control panel sets its time and date to the central station receiver time and date.

If the change moves control panel time forward, Skeds, scheduled events, or window starts and stops might be skipped. If the change moves control panel time backwards, Skeds, scheduled events, or window starts and stops might be repeated.

RPS Menu Location:
Panel Wide Parameters > Communicator > Time Synchronization

4.11 Enhanced Communication

4.11.1 Reporting Format

Default: Conettix: Modem4
Selections:
- Conettix: Modem4 - the control panel sends expanded Modem4 communication format reports to the central station receiver.
- Conettix: Contact ID - use this format when the central station receiver does not support Modem4.
- DC-09: Contact ID, TCP - the control panel sends the contact ID via SIA DC-09 TCP alarm transmission protocol to receivers and applications.
- DC-09: Contact ID, UDP - the control panel sends the contact ID via SIA DC-09 UDP alarm transmission protocol to receivers and applications.
- DC-09: SIA, TCP - the control panel sends SIA communication format reports via the SIA DC-09 TCP alarm transmission protocol to receivers and applications.
- DC-09: SIA, UDP - the control panel sends SIA communication format reports via the SIA DC-09 UDP alarm transmission protocol to receivers and applications.

Select the reporting format the control panel uses to send reports to the central station receiver.

Notice!
DC-09 report format selections are not available when European application is not enabled (set to No) in Compliance Settings.

Notice!
Contact ID does not support Time Syncronization
If you select Contact ID, you must set the *Time Synchronization, page 67* parameter to No.

Notice!
The recommended Receiver Supervision Time setting is 300 Seconds or longer when using DC09: SIA, TCP alarm transmission protocol for Reporting Format.

RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > Reporting Format

4.11.2 Receiver

Default: N/A
Configure reporting destinations to use up to 4 different Receivers (A-D).
Selections:
- A
- B
- C
- D

To identify destinations using a single Receiver, assign a shared A, B, C, or D label. To identify receivers that are different, assign a unique A, B, C, or D label.

RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > Receiver

4.11.3 Network Address

Default: Blank
Selections: IPv4 Address (0.0.0.0 to 255.255.255.255) or Hostname (Up to 255 Characters)
To route events to an IP Address (in a Private Local or Wide Area Network application), select a Destination (Destination 1 – Destination 4) and enter the IP Address for that Destination here.

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

4.11.4 Port Number

Default: 7700
Selections: 1 to 65,535
For IP communications with a central station receiver in typical installations, keep the Port at the default.

Notice!
Limit unwanted traffic, choose a port number greater than 1023
If you choose to change the port number from the default, select a port number above 1023 to decrease unwanted network traffic.

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > Port Number (Destination 1 to 4)

4.11.5 Receiver Supervision Time

Default: 4 Hours - Medium Security
Selections:
- 200 Seconds - UL1610
- 300 Seconds - NFPA 72 2010
- 1 Hour - NFPA 72 2013
- 4 Hours - Medium Security
- 24 Hours - Daily
- 25 - Hours
- 90 Seconds - High Security-UL 2050
- No Polling
- 95-195, 205-295, 305-1275 Seconds - selections available in 5 second intervals
- 2, 3, 5-23, 26-255 Hours
- Custom

With the exception of the Custom selection, the Receiver Supervision Time selection automatically sets the Poll Rate, ACK Wait, and Retry Count parameters.
The Poll Rate, ACK Wait Time, and Retry Count parameters together configure the supervision of network connections to the central station receiver for Destinations 1 to 4.

Notice!
The recommended Receiver Supervision Time setting is 300 Seconds or longer when using DC09: SIA, TCP alarm transmission protocol for Reporting Format.

The Poll Rate parameter sets the amount of time between the heartbeat polls the control panel sends to the central station receiver.
The ACK Wait parameter sets the length of time the control panel waits for the central station receiver to send the acknowledgment (ACK) of a heartbeat poll.
If the acknowledgment is not received, the control panel resends the heartbeat poll the number of times entered in Retry Count parameter. When the resend count is reached, the control panel makes a Comm Fail ## event. (Refer to the table below for the correct ## value.)

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

Even after Comm Fail ## event, the control panel continues to re-send the heartbeat poll every 10 seconds until it receives an acknowledgement.
When the control panel receives an acknowledgement from the central station, the control panel returns to the normal poll rate.

More than one network destination
When more than one network destination is configured, the control panel uses them successively. For example, if acknowledgement from Destination 1 is not received within 10 seconds, the control panel moves to Destination 2 to send the heartbeat poll, and then waits for the ACK before returning to SDI Destination 1 to resend the heartbeat poll.
If heartbeat polls sent by an SDI Destination, and ACK Wait Time (Destinations1 to 4) is exceeded, a COMM FAIL ## event occurs. When this event occurs, all events routed to this destination go immediately to the backup destination.

Notice!
When sending reports to a central station receiver over a network destination, set this parameter to a non-zero value. Failure to program a value into this parameter could prevent a failed network communication destination 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.

The first time you select Custom, the default value for the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71*, and *Retry Count, page 72* parameters is zero. Once you change these parameters from the default, RPS retains the values even if you change the Receiver Supervision Time parameter from the Custom selection. If Custom is reselected the Poll Rate, ACK Wait and Retry Count parameters are reset to the saved values.

Notice!
Receiver Supervision Time setting is critical to optimized cellular service
To prevent monthly over charges and ensure this parameter is set correctly, refer to *Configuring for Cellular Service, page 272*.

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

4.11.6 Poll Rate (sec.)

Default: 12600 (when the Receiver Supervision Time parameter set to the default 4 hours, 0 when the Receiver Supervision Time parameter is first set to Custom)
Selections: (seconds)
- 0 - the ‘heartbeat’ poll is disabled.
- 5 to 65534 - enables the poll rate for the amount of time programmed here (in seconds).
- 65535 - the 'heartbeat' poll occurs once a day.

The Receiver Supervision Time parameter must be set to Custom to edit this Poll Rate parameter. Enter the interval (in seconds) the control panel sends a heartbeat poll to the central station receiver.
- 5 minutes = 300 seconds
- 1 hour = 3600 seconds
- 12 hours = 43,200 seconds
- 18 hours = 64,800 seconds

Notice!
To edit the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71* and *Retry Count, page 72* parameters, set the *Receiver Supervision Time, page 69* parameter to Custom.
The first time you select Custom, the default value for the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71*, and *Retry Count, page 72* parameters is zero. Once you change these parameters from the default, RPS retains the values even if you change the Receiver Supervision Time parameter from the Custom selection. If Custom is reselected the Poll Rate, ACK Wait and Retry Count parameters return to the saved values.

RPS Menu Location
Panel Wide Parameters > Enhanced Communications > Poll Rate

4.11.7 ACK Wait Time (sec.)

Default: 300 (when the Receiver Supervision Time parameter set to the default 4 hours, 0 when the Receiver Supervision Time parameter is first set to Custom)
Selections: 5 to 65535 (seconds)
The Receiver Supervision Time parameter must be set to Custom to edit this ACK Wait Time parameter. Enter the time the control panel waits for an acknowledgement (ACK) from the central station receiver for heartbeat polls or reports (events). For reports, the control panel waits a maximum of 15 seconds before sending the next attempt.

Notice!
To edit the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71* and *Retry Count, page 72* parameters, set the *Receiver Supervision Time, page 69* parameter to Custom.
The first time you select Custom, the default value for the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71*, and *Retry Count, page 72* parameters is zero. Once you change these parameters from the default, RPS retains the values even if you change the Receiver Supervision Time parameter from the Custom selection. If Custom is reselected the Poll Rate, ACK Wait and Retry Count parameters return to the saved values.

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

4.11.8 Retry Count

Default: 5 (when the Receiver Supervision Time parameter set to the default 4 hours, 0 when the Receiver Supervision Time parameter is first set to Custom)
Selections:
0 - continuous retries. No comm failure events for heartbeat poll.
1 to 255 - number of of times the control panel resends the heartbeat poll.
Enter the number of times the control panel resends the heartbeat poll before making a COMM FAIL SDI2 ## event. (Refer to the table below for the correct ## value.)

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

Notice!
To edit the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71* and *Retry Count, page 72* parameters, set the *Receiver Supervision Time, page 69* parameter to Custom.
The first time you select Custom, the default value for the *Poll Rate (sec.), page 71*, *ACK Wait Time (sec.), page 71*, and *Retry Count, page 72* parameters is zero. Once you change these parameters from the default, RPS retains the values even if you change the Receiver Supervision Time parameter from the Custom selection. If Custom is reselected the Poll Rate, ACK Wait and Retry Count parameters return to the saved values.

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

4.11.9 AES Key Size

Default: No Encryption
Selections:
– No Encryption
– 128 bits - 16 bytes
– 192-bit - 24 bytes
– 256-bit - 32 bytes
Select the AES key size.

RPS Menu Location:
Panel Wide Parameters > Enhanced Communications > AES Key Size

4.11.10 AES Encryption Key

Default: <Default> (Represents Key ID 1 listed in RPS Config > System > Global to all Accounts > Encryption Key)
Selections: Thirty-two hexadecimal characters represented by an ID (01 to 100).
Use this parameter to configure each receiver destination with a unique AES encryption key. The AES Encryption Key is based on *AES Key Size, page 72*. For the encryption key configuration, only Key ID & Name is displayed.
If two or more network destinations have the same network address, then RPS notifies the operator to use the same encryption key for those network destinations.
AES key strings are configured in Config > System > Global to all Accounts > Encryption Key

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

4.12 SDI2 RPS / Enhanced Communication

4.12.1 Enable Enhanced Communication?

Default: Yes
Selections:
– Yes - enables reporting using an IP communicator (onboard, plug-in cellular, or SDI2).
– No - disables reporting using an IP communicator.

To enable reporting using an IP communicator (onboard, plug-in cellular, or SDI2), set this parameter to Yes.
Set the *Primary Destination Device, page 65* or *Backup Destination Devices, page 66* for at least one Route Group to an Onboard IP, Plug-in Cellular, or SDI2 device.

4.12.2 Answer RPS Over Network?

Default: Yes
Selections:
– Yes - enables automatic RPS initiated connections through the onboard Ethernet communicator or a network interface module on the SDI2 bus.
– No - prevents automatic RPS initiated connections over the network.

If set to No, RPS initiated connections can be accepted at a keypad by selecting Answer from the RPS menu (Actions > RPS > Answer).

Notice!
Service Mode allows RPS connections over network
When the control panel is in service mode, the control panel automatically accepts RPS initiated connections over the network, even if this parameter is set to No.
To place the control panel in installer mode, press and hold the control panel RESET button until the Heartbeat LED flashes fast. Keypads show SERVICE MODE and prompt for the installer passcode. Enter the installer passcode and press [ENTER].

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

4.12.3 RPS Address Verification

Default: No

Selections:
- Yes - the control panel verifies that the IP address RPS is attempting to connect from matches the RPS Network Address.
- No - allows RPS to connect to the control panel from any IP address.

Further information
RPS Network Address, page 74

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

4.12.4 RPS Network Address
Default: Blank
Selections: IPv4 address or Hostname
Enter the IP address or hostname for RPS.
Contact your network administrator to determine the IP Address or hostname your RPS computer is connected to.

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

4.12.5 RPS Port Number
Default: 7750
Selections: 1 – 65535
Enter the destination UDP port for control panel-initiated RPS network sessions.

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

4.13 Power Supervision

4.13.1 AC Fail Time
Default: 01:00
Selections: 00:01 to 90:00 (Minutes:Seconds)
Enter the time that the AC power is off before the control panel sends an AC Fail report.

RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Fail Time

4.13.2 Resend AC Fail
Default: No Reports
Selections:
- No Report -do not resend AC Fail report.
- After 6 Hours - resend AC Fail report to central station after 6 hours.
- After 12 Hours - resend AC Fail report to central station after 12 hours.

The time without AC power restoring the panel waits before resending an AC Fail report.

RPS Menu Location
Panel Wide Parameters > Power Supervision > Resend AC Fail

4.13.3 AC Fail Display
Default: 60
Selections: 10 to 300 (seconds) (increments of 5)
The time the control panel waits before keypads display AC Fail.

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

4.13.4 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.
The control panel waits the time set in the AC Fail Time parameter before sending AC Fail reports.

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

4.13.5 AC Tag Along

Default: Yes
Selections:
– Yes - send only if any other event occurs while AC is off-normal.
– No - do not send AC Fail reports as tag along events.
The control panels sends tag along AC Fail reports only if any other event occurs while AC is off-normal.

RPS Menu Location
Panel Wide Parameters > Power Supervision > AC Tag Along.

4.13.6 AC / Battery Buzz

Default: No
Selections:
– Yes - sound panel-wide trouble tone at all keypads on AC fail, battery low, and battery missing.
– No - do not sound panel-wide trouble tone on AC fail, battery low, and battery 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

4.13.7 Battery Fail / Restoral Report

Default: Yes
Selections:
– Yes - the control panels sends battery fail and restoral reports to the central station receiver.
– 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.
Battery fail and restoral reports are routed to destination devices assigned to Route Groups configured for Diagnostic Reports.
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.

4.14 RPS Parameters

4.14.1 RPS Passcode

Default: 999999
Selections: 6 to 24 alphanumeric characters (Do not use spaces in the passcode. The passcode is case-sensitive.)
This is the passcode that RPS will save and use to establish a connection to the panel.

Notice!
UL 2610 requirement
For UL 2610 compliance, the password length must be at least 6 characters and contain a combination of numbers, letters and symbols.

Notice!
IMPORTANT! All panels are manufactured with a factory default passcode. Set and synchronize a new, non-default RPS Passcode in your panel account configuration to secure access and control connections to your panel.

For the initial panel connection, the factory default passcode must be used as the RPS Passcode in the connection window. Once connected, users can modify the RPS Passcode through configuration or synchronization.

– For new panels with Firmware v3.09+ and B465 modules with Firmware v2.09+, use the factory default Cloud ID passcode. Locate this panel unique passcode on the printed label of each physical panel.
– For legacy panels with Firmware prior to v3.09 and B465 modules with Firmware prior to v2.09, use the factory default passcode of 999999.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Passcode

4.14.2 Log % Full

Default: 0
Selections: 0 (disabled), 1 to 99 (%)
When the control panel log is this percent full, the control panel adds a Log Threshold event to the log and sends a report to the central station receiver.
Enter 0 to disable Log Threshold and Log Overflow events (no events added to log or reports sent).
The Log Threshold report alerts the central station to connect to the control panel and copy the panel log before events are overwritten.
The control panel continues to log events after sending the Log Threshold report. When it reaches 100% capacity (log is full and stored events are overwritten), the control panel makes a local LOG OVERFLOW event.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > Log % Full.

4.14.3 Contact RPS if Log % Full

Default: No

Selections:

– Yes - the control panel automatically contacts RPS and when the “Log % Full” threshold is reached.

– No - the control panel does not automatically contact RPS when the “Log % Full” threshold is reached.

RPS Menu Location

Panel Wide Parameters > RPS Parameters > Contact RPS if Log % Full.

4.14.4 RPS Call Back

Default: No

Selections:

– Yes - after the control panel receives the RPS passcode from RPS, it disconnects, and dials the RPS Phone # to establish a connection with RPS.

– No - the control panel connects to RPS after the RPS passcode is verified.

When using the RPS Callback function with DTMF dialing, enter a "C" as the last digit in the RPS phone number.

Further information

RPS Phone #, page 78

RPS Menu Location

Panel Wide Parameters > RPS Parameters > RPS Call Back

4.14.5 RPS Line Monitor

Default: Yes

Selections:

– Yes - if the control panel hears the RPS Line Monitor tone after an answering machine, other device, or person answers an incoming call, the control panel seizes the phone line.

– No - the control panel does not seize the phone line to connect with RPS when it hears the RPS Line Monitor tone.

You must set *Answer Armed, page 77* and/or *Answer Disarmed, page 78*, and the control panel must be in the related armed state (armed or disarmed).

If you set this RPS Line Monitor parameter to Yes, set answering machines that share the phone line with the control panel to pick up after two or more rings.

If *RPS Call Back, page 77* is set to Yes, the control panel hangs up the phone after the it receives the RPS passcode, then it calls the RPS phone number.

Notice!

Set RPS Line Monitor to No if the control panel falsely seizes the phone line

False seizures of the phone line indicate that a device sharing the phone line is using a tone with the same frequency as the RPS Line Monitor tone.

RPS Menu Location

Panel Wide Parameters > RPS Parameters > RPS Line Monitor

4.14.6 Answer Armed

Default: 7

Selections: 0 to 15 (rings)

– 1 to 15 - the control panel waits this number of rings to answer (seize the phone line) when all Areas are armed All On. If the control panel shares the phone line with an answering machine, enter a number 2 rings higher than the number for the answering machine.
– 0 (disabled) - the control panel does not answer (seize the phone line) when all Areas are armed All On.

Notice!
For RPS, Part On is a disarmed state.

If any area is Part On or disarmed (Off), the control panel uses *Answer Disarmed, page 78* ring counter.

Notice!
PSTN requirement for Australia / New Zealand, disable RPS answer armed/disarmed
If you set the Panel Wide Parameters > Phone Parameters > PSTN Compatibility parameter to Australia or New Zealand, you must set this Answer Armed and the Answer Disarmed parameter to 0 (disabled).

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

4.14.7 Answer Disarmed

Default: 7
Selections: 0 to 15 (rings)
– 1 to 15 - the control panel waits this number of rings to answer (seize the phone line) when at least one Area is disarmed (Off) or armed Part On. If the control panel shares the phone line with an answering machine, enter a number 2 rings higher than the number for the answering machine.
– 0 (disabled) - the control panel does not answer (seize the phone line) when at least one Area is disarmed (Off) or armed Part On.

Notice!
For RPS, Part On is a disarmed state.

Notice!
PSTN requirement for Australia / New Zealand, disable RPS answer armed/disarmed
If you set the Panel Wide Parameters > Phone Parameters > PSTN Compatibility parameter to Australia or New Zealand, you must set the Answer Armed and this Answer Disarmed parameter to 0 (disabled).

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

4.14.8 RPS Phone

Default: Blank
Selections: Up to 24 characters
Enter the phone number the control panel dials to connect to RPS.

The control panel calls RPS for the following events:
- *Log % Full, page 76* threshold is achieved (if enabled).
- RPS calls the control panel and the *RPS Call Back, page 77* parameter is set to Yes.
- At a keypad, a user selects MENU > Actions > RPS > Call Via Phone (only one attempt is made).

If this parameter is blank, the control panel does not dial a phone number for RPS.
For further information on the characters the control panel can dial, refer to *Phone Destination 1 (to 4), page 31*.

RPS Menu Location
Panel Wide Parameters > RPS Parameters > RPS Phone

4.14.9 RPS Modem Speed

Default: 1200
Selections:
- 300
- 1200
- 2400

Set 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.

4.15 Miscellaneous

4.15.1 Duress Type

Default: 0
Selections:
- 0 - disabled, no duress alarm reports.
- 1 - +1, users add 1 to the last digit of their passcode to send a duress alarm report when they enter the passcode at a keypad.
- 2 - +2, users add 2 to the last digit of their passcode to send a duress alarm report when they enter the passcode at a keypad.
- 3 - the control panel sends a duress alarm report whenever a user assigned to an Authority Level with Send Duress set to yes enters their passcode at a keypad.

For example when Duress Type is set to 1 (+1):
- 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.

For example when Duress Type is set to 2 (+2):
- 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.

When Duress type is set to 3, and users assigned to an Authority Level with *Send Duress, page 178* set to Yes, enter their passcode at a keypad, the control panel sends a Duress alarm.
Duress alarm reporting is enabled or disabled by area in Area Parameters, *Duress Enable, page 99*.

Notice!
SIA CP-01 False Alarm Reduction requirement
To comply with SIA CP-01 False Alarm Reduction, set this parameter to 3. Refer to SIA CP-01 Verification for more information

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Duress Type.

4.15.2 Cancel Reports

Default: Yes
Selections:
– Yes - send Cancel, Fire Cancel and Gas Cancel reports.
– No - do not send Cancel, Fire Cancel and Gas Cancel reports.
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.

Notice!
SIA CP-01 False Alarm Reduction requirement
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
Panel Wide Parameters > Miscellaneous > Cancel Reports

4.15.3 Call for Service Text - First Language

Default: Contact your dealer
Selections: Enter up to 32 characters of text, numbers, symbols, or spaces.
The Call for Service text shows at keypads for system trouble events.
Spaces before, after and within a string of text are included in the 32 character limit.
Keypads display the first 20 characters, and then scroll any remaining characters across the display one time. To scroll again, press [ESC].
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 - English

4.15.4 Call for Service Text - Second Language

Default: Blank
Default: Contact your dealer
Selections: Enter up to 32 characters of text, numbers, symbols, or spaces.
The Call for Service text shows at keypads for system trouble events.
Spaces before, after and within a string of text are included in the 32 character limit.
Keypads display the first 20 characters, and then scroll any remaining characters across the display one time. To scroll again, press [ESC].
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

4.15.5 On Site Authorization for Firmware Update

Default: No
Selections:
– Yes - require on-site authorization for firmware update.
– 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.

Notice!
Remote firmware updates must be authorized on-site for UL listed systems
Set this parameter to "Yes" for UL listed systems.

Perform a full system test whenever firmware is updated locally or remotely.

Further information
Firmware Update, page 181

RPS Menu Location
Panel Wide Parameters > Miscellaneous > On-Site Authorization for Firmware Update.

4.15.6 System Tamper Response

Default: Trouble
Selections:
– Trouble - system tampers are trouble events.
– Always Alarm - system tampers are audible and visible alarm events.
– Alarm while Disarmed - when at least one area is armed, system tampers are silent and invisible alarm events. When all areas are disarmed, system tampers are audible and visible alarm events.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > System Tamper Response

4.15.7 Enclosure Tamper Enable

Default: No
Selections:
– Yes - enable the control panel tamper input.
– No - disable the control panel tamper input.
When the enclosure tamper input is enabled, the control panel creates an enclosure tamper event when the control panel enclosure is opened.
Tamper events do not affect the arming or disarming process.
When you change the parameter from No to Yes, the control panel does not create tamper events until it sees the tamper input in the normal state (enclosure door is closed).
If you change this parameter from Yes to No and there is an existing enclosure tamper event, the event is cleared. No restoral event is logged or reported.
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 in the normal state.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Enclosure Tamper Enable

4.15.8 Fire and Gas Summary Sustain

Default: Yes

Selections:

– Yes - Summary Fire and Summary Gas outputs remain active after the Alarm Silence command.

– No - Summary Fire and Summary Gas outputs are active until all silenced fire or gas points in the system return to normal.

Set to Yes to keep fire or gas strobes active after fire or gas bells are silenced.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Fire and Gas Summary Sustain

4.15.9 Fire Supervision Event Type

Default: Fire Supervision Restoral

Selections:

– Fire Trouble Restoral - the control panel send a FIRE TROUBLE RESTORE report when a Fire Supervision point restores to normal.

– Fire Alarm Restoral - the control panel sends a FIRE ALARM RESTORE report when a Fire Supervision point restores to normal.

– Fire Supervision Restoral - the control panel sends a FIRE SUPERVISION RESTORE report when a Fire Supervision point restores to normal.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Fire Supervision Event Type

4.15.10 Fire and Gas Resound

Default: None

Selections:

– None - keypads do not re-sound the trouble tone.

– Noon - keypads re-sound the trouble tone at 12:00 P.M. (noon) if any fire or gas point that falls in scope of a keypad is in an off-normal state.

– Midnight - keypads re-sound the trouble tone at 12:00 A.M. (midnight) if any fire or gas point that falls in scope of a keypad is in an off-normal state.

When resound is enabled, previously acknowledged and silenced fire or gas trouble events automatically resound the trouble tone.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Fire and Gas Resound

4.15.11 Early Ambush Time

Default: 10

Selections: 5 to 30 (1-minute increments)

Enter the amount of time for a user to enter a second passcode at the keypad when disarming (turning OFF). If a second passcode is not entered before Early Ambush Time ends, the control panel creates a Duress event.

Refer to the Area Parameter, *Early Ambush?, page 102* to enable the Early Ambush feature.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Early Ambush Time

4.15.12 Second Ambush Code

Default: Unique

Selections:
- Unique - the second passcode entered for the Early Ambush process must be different from the first passcode entered to disarm the area.
- Any - the second passcode entered for the Early Ambush can be different from the first passcode entered to disarm the area, or it can be the same passcode.

Refer to the Area parameter, *Early Ambush?, page 102* process.

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

4.15.13 Abort Window

Default: 30 sec
Selections: 15 to 45 (seconds) (1-sec increments)
Enter the number of seconds the control panel waits before sending an alarm report for a point assigned to a Point Profile with the Alarm Abort feature enabled.
Refer to *Alarm Abort, page 215* for a description of the Alarm Abort feature.

Notice!
UL requirement
To meet UL requirements, the combined *Entry Delay, page 206* and Abort Window time must not exceed 60 sec.

Notice!
SIA CP-01 requirement
For SIA CP-01 Compliance, Abort Window is a required parameter.

If a users silences the alarm before the Abort Window ends, the alarm report is aborted (not sent) and the keypad shows an optional message (Refer to *Abort Display, page 119*).
This feature does not apply to fire alarms or invisible point alarms.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Abort Window

4.15.14 Passcode Length

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

When set to 3, 4, 5, or 6 digits, passcode length is fixed for all passcodes. Users do not need to press the Enter key after entering their passcode.
When set to Disabled, passcode length is not fixed. Individual passcodes can be 3 to 6 digits in length. Users must press the Enter key after entering their passcode.

Notice!
SIA CP-01 requirement
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 changing the passcode length creates duplicate or unusable passcodes, a WARNING! Duplicate / Unusable Passcodes Present window opens.
Duplicated passcodes show in bold red.

Unusable passcodes (their length is under or over the length entered in this parameter), show in bold blue.

To correct duplicated or unusable passcodes:

1. Select the passcode (click the cell in the User Passcode column).
2. Press the [Backspace] key on your keyboard to clear the cell.
3. Enter the new passcode.
4. Click Save corrected passcodes to save your changes. All passcodes marked as duplicate or unusable must be fixed before you click OK.
   - or -
   Click Disable passcode length and store the data in this account. This option sets the Passcode Length parameter to Disabled and allows you to save passcodes of varying lengths in the RPS account.

Notice!

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?"

Similar and Duplicate Passcodes

- 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

4.15.15 Swinger Bypass Count

Default: 2

Selections: 1 to 4

This parameter sets the maximum number of faults allowed on a controlled point within an arming cycle before the point is swinger bypassed.

Notice!

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.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Swinger Bypass Count

4.15.16 Remote Warning

Default: No

Selections:

– Yes - when the area is remotely armed, the control panel pulses the alarm bell once. When the area is remotely disarmed, it pluses the alarm bell twice.
– No - No remote warning for remote arming.

Users can remotely arm or disarm using a RADION keyfob, Inovonics Pendant Transmitter, keyswitch, or remote software.

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

Further information
Alarm Bell, page 135

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Remote Warning

4.15.17 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 AC frequency (from primary power source) to regulate its clock time.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Crystal Time Adjust

4.15.18 Part On Output

Default: No
Selections:
– Yes - the Fail to Close output function becomes Part On output function. Part On outputs activate 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.

When this Part On Part On parameter is set to Yes, Use the *Early Area Armed Output, page 85* parameter to select if the Part On output activates at the beginning of exit delay, or at the end of exit delay. The default is that the output activates at the end of exit delay.

Further information
Fail to Close/Part On Armed, page 136

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Part On Output

4.15.19 Early Area Armed Output

Default: No
Selections:
– Yes - activates the Area Armed output or Part On output at the start of Exit Delay time.
– No - activates the Area Armed output or Part On output at the end of Exit Delay time.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Early Area Armed Output

4.15.20 Daylight Saving Time

Default: US DST

Selections:

– No DST - The control panel does not adjust its clock for daylight saving time.
– US DST
– Brazil DST
– Mexico DST
– Paraguay DST
– Australia DST
– New Zealand DST
– EU DST

The control panel clock follows daylight saving time rules for the countries shown.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Daylight Saving Time

4.15.21 Date Format

Default: mm dd yy

Selections:

– mm dd yy
– dd mm yy
– yy mm dd

Choose how the month, day, and year are delimited (separated) in the Date Delimiter parameter.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Date Format

4.15.22 Date Delimiter

Default: / (forward slash)

Selections:

– / (forward slash)
– . (period)
– - (dash)

Select how the month (mm), day (dd), and year (yy) are delimited (separated).
Choose how the month, day, and year are displayed in the Date Format parameter.

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Date Delimiter

4.15.23 Time Format

Default: 12 hour (with AM/PM)

Selections:

– 12 hour (with AM/PM)
– 24 hour

Choose the 12 hour format, hh:mm AM (or PM), or 24 hour format, hh:mm (00:00 to 23:59).

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Time Format

4.15.24 Time Zone

Default: UTC-05:00 (Eastern Time, US & Canada)

Selections: Time Zones and UTC
This parameter identifies the time zone where the control panel is installed.
(UTC-12:00) International Date Line West
(UTC-11:00) Midway Island, Samoa
(UTC-10:00) Hawaii
(UTC-09:00) Alaska
(UTC-08:00) Pacific Time (US & Canada)
(UTC-08:00) Tijuana, Baja California
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
(UTC-06:00) Central America
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Guadalajara, Mexico City, Monterrey
(UTC-06:00) Saskatchewan
(UTC-05:00) Bogota, Lima, Quito
(UTC-05:00) Eastern Time (US & Canada)
(UTC-05:00) Indiana (East)
(UTC-04:30) Caracas
(UTC-04:00) Asuncion
(UTC-04:00) Atlantic Time (Canada)
(UTC-04:00) Georgetown, La Paz, San Juan
(UTC-04:00) Manaus
(UTC-04:00) Santiago
(UTC-03:30) Newfoundland
(UTC-03:00) Brasilia
(UTC-03:00) Buenos Aires
(UTC-03:00) Cayenne
(UTC-03:00) Greenland
(UTC-03:00) Montevideo
(UTC-02:00) Mid-Atlantic
(UTC-01:00) Azores
(UTC-01:00) Cape Verde Is.
(UTC) Casablanca
(UTC) Coordinated Universal Time
(UTC) Dublin, Edinburgh, Lisbon, London
(UTC) Monrovia, Reykjavik
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(UTC+01:00) West Central Africa
(UTC+02:00) Amman
(UTC+02:00) Athens, Bucharest, Istanbul
(UTC+02:00) Beirut
(UTC+02:00) Cairo
(UTC+02:00) Harare, Pretoria
(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC+02:00) Jerusalem

(UTC+02:00) Minsk
(UTC+02:00) Windhoek
(UTC+03:00) Baghdad
(UTC+03:00) Kuwait, Riyadh
(UTC+03:00) Moscow, St. Petersburg, Volgograd
(UTC+03:00) Nairobi
(UTC+03:00) Tbilisi
(UTC+03:30) Tehran
(UTC+04:00) Abu Dhabi, Muscat
(UTC+04:00) Baku
(UTC+04:00) Port Louis
(UTC+04:00) Yerevan
(UTC+04:30) Kabul
(UTC+05:00) Ekaterinburg
(UTC+05:00) Islamabad, Karachi
(UTC+05:00) Tashkent
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
(UTC+05:30) Sri Jayawardenepura
(UTC+05:45) Kathmandu
(UTC+06:00) Almaty, Novosibirsk
(UTC+06:00) Astana, Dhaka
(UTC+06:30) Yangon (Rangoon)
(UTC+07:00) Bangkok, Hanoi, Jakarta
(UTC+07:00) Krasnoyarsk
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
(UTC+08:00) Irkutsk, Ulaan Bataar
(UTC+08:00) Kuala Lumpur, Singapore
(UTC+08:00) Perth
(UTC+08:00) Taipei
(UTC+09:00) Osaka, Sapporo, Tokyo
(UTC+09:00) Seoul
(UTC+09:00) Yakutsk
(UTC+09:30) Adelaide
(UTC+09:30) Darwin
(UTC+10:00) Brisbane
(UTC+10:00) Canberra, Melbourne, Sydney
(UTC+10:00) Guam, Port Moresby
(UTC+10:00) Hobart
(UTC+10:00) Vladivostok
(UTC+11:00) Magadan, Solomon Is., New Caledonia
(UTC+12:00) Auckland, Wellington
(UTC+12:00) Fiji, Marshall Is.
(UTC+12:00) Petropavlovsk-Kamchatsky
(UTC+13:00) Nuku'alofa

RPS Menu Location

Panel Wide Parameters > Miscellaneous > Time Zone

4.15.25 Custom Text Format

Notice!
Read only parameter
You cannot change this parameter.
RPS automatically sets the Custom Text Format when you set the Panel Data - View > Panel Info > First Language and Second Language parameters.

Selections (read only):
- Standard - RPS sets this Custom Text Format parameter to Standard (Latin-1 character set) when both the Panel Data - View > Panel Info > First Language and Second Language parameters are set to English, Dutch, French, German, Hungarian, Italian, Portuguese, Spanish or Swedish.
- Extended - RPS sets this Custom Text Format parameter to Extended (UTF-8 Unicode character set) when the panel language is set to Chinese, Polish, or Greek or if an account is connected to a panel where the language is already set to Chinese, Polish, or Greek.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Custom Text Format

4.15.26 Minimum TLS version
Default: Highest Avail
Selections:
- Highest Avail
- TLS 1.0
- TLS 1.1
- TLS 1.2

Select the minimum supported Transport Layer Security (TLS) version to use for panel and communicator connections. This parameter allows support for the selected version and higher versions. The default is the highest available version of TLS currently available.

RPS Menu Location
Panel Wide Parameters > Miscellaneous > Minimum TLS version

4.16 Personal Notification Destinations

4.16.1 Description
Default: Blank (text is for reference only)
Selections: 0 to 32 characters in length
Enter text to identify the personal notification device or notification addressee.

RPS Menu Location
Panel Wide Parameters > Personal Notification > Personal Notification Destinations > Description.

4.16.2 SMS Phone # / email address
Default: Blank
Selections: Up to 255 alphanumeric characters
Enter either a destination phone number to receive SMS text notifications, or an email address to receive email messages.

SMS Phone #

The control panel sends personal notifications to a cellular device when the destination is a cellular telephone number containing only numbers 0-9. Hyphens are not allowed.

Email Address

The control panel sends personal notifications to email accounts when the destination is an email address.

Notice!

Personal notification not sent for incorrect entries

If your entry is neither a correct phone number nor a correct email address, the control panel does not send a personal notification message. The control panel logs an SMS send error.

RPS Menu Location

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

4.16.3 User Language

Default: 1: [language set as First Language in Panel Data - View]

Selections:

– 1: [language set as First Language in Panel Data - View]
– 2: [language set as Second Language in Panel Data - View]

Select the language personal notification messages are sent in.

First and Second languages are programmed during panel account setup in the Panel Data - View.

RPS Menu Location

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

4.16.4 Method

Default: Plug in Cellular SMS

Selections:

– None
– Plug-in Cellular SMS - may be selected if you have a B44x plug-in cellular module.
– Plug-in Cellular Email - may be selected if you have a B44x plug-in cellular module.
– Bus Device Cellular SMS - may be selected if you have a B450 v2 module.
– Bus Device Email - may be selected if you have a B450 v2, or a B426 v3 module.
– On-board Ethernet Email - may be selected if your connection is on-board IP.

Select the Personal Notification destination and destination device used to send the notification.

RPS Menu Location

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

4.17 Personal Notification Reports

IMPORTANT CELLULAR SERVICE INFORMATION

Refer to *Configuring for Cellular Service, page 272* for important information regarding how to set up your control panel to ensure proper cellular communication with the central station receiver.

Use this parameter to assign Personal Notifications to Destinations and Route Groups.
The control panel sends personal notifications to a cellular device when the destination is a cellular telephone number.
The control panel sends personal notifications to email accounts when the destination is an email address.

Notice!
Personal notification not sent for incorrect destination
If the destination is not set to a correct phone number or a correct email address, the control panel does not send the personal notification message. The control panel logs an SMS send error.

Notice!
Cellular IP for Primary Destination Device or Backup Destination Device not required
You are not required to set the Primary Destination Device or Backup Destination 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

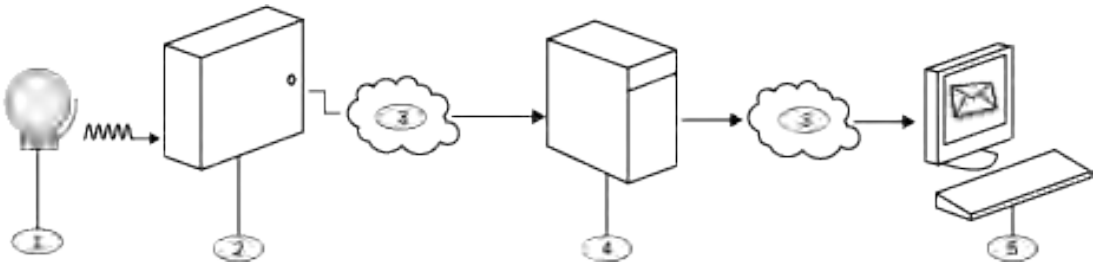
4.18 Personal Notification Routing Attempts

Default: 3
Selections: 1-6
Set the number of attempts the control panel makes to send a personal notification.

RPS Menu Location
Panel Wide Parameters > Personal Notification > Personal Notification Routing Attempts

4.19 Email Server Configuration

You can configure the control panel to send personal notifications to up to 16 email addresses.
When an event occurs, the control panel transmits a report across an IP network to an email server. The SMTP (Simple Mail Transfer Protocol) email server translates the incoming data into text and then pushes it out to the destinations you configured. This is a one-way communication from the control panel to the user.



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

Setting up an Email Account

To setup an email account that sends emails to the Personal Notification Destinations:

1. Register for an email account from an email provider (example: Google, Yahoo, AOL, Microsoft).
2. Choose a user name that makes it easy for the individuals receiving the notifications to identify which emails are coming from the control panel (example: panelacctstore52).
3. Enter the address associated with the SMTP email server you chose in the Email Server Name/Address parameter.
4. Enter the user name you specified when registering for this account in the Authentication User Name parameter.
5. Enter the password you specified when registering for this account in the Authentication Password parameter.

4.19.1 Email server name/address

Default: Blank

Selections: Domain name or IP address

Enter either the domain name or address for the SMTP (Simple Mail Transfer Protocol) email server for your chosen provider.

The control panel uses the server's domain name (or address) to sent personal notification messages from the control panel to designated personal notification email addressees.

SMTP Email Servers

Refer to the table below for the some popular email providers and their server's domain name. If your provider does not appear in the table, contact them for their domain name (or IP address).

Email provider	Domain name
1&1	smtp.1and1.com
Airmail	mail.airmail.net
AOL	smtp.aol.com
AT&T	outbound.att.net
Bluewin	smtpauths.bluewin.ch
BT Connect	mail.btconnect.tom
Comcast	smtp.comcast.net
Earthlink	smtpauth.earthlink.net
Gmail	smtp.gmail.com

Email provider	Domain name
Gmx	mail.gmx.net
HotPop	mail.hotpop.com
Libero	mail.libero.it
Lycos	smtp.lycos.com
O2	smtp.o2.com
Orange	smtp.orange.net
Outlook.com (former Hotmail)	smtp.live.com
Tin	mail.tin.i
Tiscali	smtp.tiscali.co.uk
Verizon	outgoing.verizon.net
Virgin	smtp.virgin.net
Wanadoo	smtp.wanadoo.fr
Yahoo	smtp.mail.yahoo.com

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location

Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Name/Address

4.19.2 Email server port number

Default: 25

Selections: 1-65535

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.

Examples of common providers, email servers, ports, and security:

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	AT&T outbound.att.net	465	Encrypted
Comcast	smtp.comcast.net	465	Encrypted
Time Warner	smtp-server.<region>.rr.com	25	Authenticate

RPS Menu Location
Panel Wide Parameters > Personal Notification > Email Server Configuration > Email Server Port Number

4.19.3 Email server authentication/encryption

Default: Authenticate
Selections:
Basic - no authentication, no encryption
Authenticate - authentication required, no encryption
Encrypted - authentication required, encryption required
Select the security level required by the email server to receive messages from the control panel.
Authentication means that the email server requires an authentication user name and authentication password. This is sometimes referred to as SMTP-AUTH.
The Encryption used is Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

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

4.19.4 Authentication user name

Default: Blank
Selections: Blank, 1 to 255 characters
Enter the user name for the email account receiving personal notification email sent by the control panel.

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

4.19.5 Authentication password

Default: Blank
Selections: Blank, 1 to 49 characters
Enter the password that the SMTP server uses to send emails to the Personal Notification destinations.

RPS Menu Location
Panel Wide Parameters > Personal Notification > Email Server Configuration > Authentication Password

5 Area Wide Parameters

5.1 Area / Bell Parameters, Open / Close Options

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).

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).

The B6512 supports up to 6 areas.

5.1.1 Area Name Text (first language)

Default: Area # (# = the Area number)

Selections: Up to 32 characters of text, numbers, spaces, and symbols

Enter an Area name for display at keypads.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Name Text

5.1.2 Area Name Text (Second Language)

Default: Blank

Selections: Up to 32 characters of text, numbers, spaces, and symbols

Enter an Area name for display at keypads.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Name Text (Second Language)

5.1.3 Area On

Default:

- B6512:
  - Area 1: Yes

– Areas 2 to 6: No

Selections:
Yes - Area is enabled.
No - Area is disabled.

Notice!
UL 864 requirement
To comply with UL 864 requirements for Commercial Fire Systems, set this parameter to Yes.

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.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area On

5.1.4 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.

Notice!
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.

Notice!
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.

5.1.5 Force Arm/Bypass Max

Default: 2
Selections:
B6512 - 0 to 30
Enter the number of controlled points that can be faulted or in a bypassed state when arming the area.

Refer to *Force Arm Returnable, page 211* and *Bypass Returnable, page 211* in the Point Profile for returning a point to the system when the point returns to normal or when the area is disarmed.

Notice!
Points must have *Bypassable, page 211* set to Yes to be bypassed or force armed. Force arming does not bypass 24-hour points.

Notice!
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.

5.1.6 Delay Restorals

Default: No Delay
Selections:
No Delay - Point restoral events are logged and reported when the point physically restores.
Delay Until Bell is Silenced - Point restoral events are not logged or reported until the point has physically restored and the bell is silenced (or 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

5.1.7 Exit Tone

Default: Yes
Selections:
Yes - Sound an exit tone at all keypads during exit delay.
No - Enable/disable exit tones for keypads individually (in Keypad configuration).

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Exit Tone

5.1.8 Exit Delay Time

Default: 60
Selections: 0 to 600 (seconds, in increments of 5)
Set the amount of time users have to leave the premises without creating an alarm event after arming their system All On - Exit or Part On - Exit.
They must leave through a point assigned to a point profile that is configured for a controlled point type with a delayed alarm response (refer to *Point Response, page 195*)
Points programmed for instant alarm response generate alarms immediately, even during exit delay.

Notice!
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

5.1.9 Auto Watch

Default: Manual

Selections:
- Manual - users turn Watch Mode on and off manually from a keypad.
- On at Disarm - the control panel automatically turns Watch Mode on when the area is disarmed (turned Off).

When an area is disarmed (Off) and Watch Mode is on, the watch tone sounds at keypads when points configured as Watch Points are faulted.
Refer to *Watch Point, page 209*s for instructions on configuring points for the Watch feature.
When the area is armed Part On, only interior points configured as Watch Points sound the watch tone when they are faulted. Perimeter points report faults as alarms or troubles.
If this Auto Watch parameter is set to Manual and Watch Mode is on when the area is armed (All On or Part On, Watch Mode is on when the area is disarmed (Off).

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Watch

5.1.10 Restart Time

Default: 5
Selections: 5 to 55 (seconds) (in 1 second increments)
Set the length of time to wait for sensors to stabilize after an alarm verification point is faulted and the sensor reset has reapplied power to the sensors.
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. Alarm verification also applies to gas points.

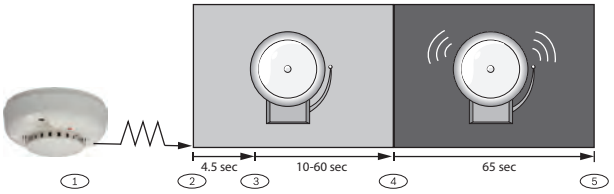
Notice!
Do not enable the Cross Point Feature in Point Profiles that are designated for fire and gas points.

Notice!
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.

Notice!
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 Profiles, page 188*. Any resettable fire or gas 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 or Gas Point, 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. When power is reapplied, the control panel ignores alarms 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

5.1.11 Duress Enable

Default: No

Selections:

– Yes - Enable Duress alarm for this area.

– No - Disable Duress alarm for this area.

Notice!

SIA CP-01 requirement

To comply with SIA CP-01, set this parameter to Yes.

If a user uses the Move command to move the keypad 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.

Further information

Refer to *Duress Type, page 79* for an explanation of Duress

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Duress Enable

5.1.12 Area Type

Default: Regular

Selections:

Regular - armed and disarmed independently of other areas.

Master - before arming a Master area, Associate areas with the same account number as the Master must be in exit delay, or armed All On Delay. Multiple Master areas can share an account number.

Associate - a Shared area account number links Associate areas with Master areas. Associate areas can be armed and disarmed independently of other Associate areas with the same account number and the Master Area.

Shared - shared areas are not linked to other areas by account number. They arm when all Associate areas in the control panel are armed All On Delay. Shared areas disarm when at least one Associate area in the control panel is not armed All On Delay (armed Part On or disarmed).

Arming Master and Associate areas

When arming a Master Area when the Associate areas are not armed, a Check Area message displays.

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

Notice!

Keypad Scope affects master arming.

Arming a Master area from a keypad with Keypad Scope set to Panel Wide or Account Wide, starts Exit Delay for all Associate areas (with the same account number).

Notice!

To use a Sked to arm a Master area, first use Skeds to arm Associate areas

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.

Notice!

RPS, Keyswitch, or Auto Close function arm Master areas without Associate areas being armed

Arming Master areas with RPS, keyswitches, or the Auto Close function does not require all Associate areas be armed.

Arming Shared and Associate areas

Arming all Associate areas arms Shared areas. As soon as the last Associate area is armed, the Shared area begins arming automatically using the Exit Delay for the Area the keypad is assigned to.

Shared areas cannot be armed using a passcode, card, keyswitch, Sked, or with RPS.

Shared areas automatically disarm when any Associate area in the control panel is disarmed.

Shared areas cannot be disarmed by passcode, card, keyswitch or with RPS.

Notice!

Arming commands require Panel Wide scope

Arming commands intended for a Shared area must be executed on a keypad with Panel Wide scope by a user with authority in all Associate areas.

When a Shared Area, is not ready to arm
If a point is faulted in the Shared area, [CHECK AREA] displays on the keypad for the last Associate area to arm.

Notice!
Associate area keypad Scope must include Shared areas
To view a Shared area's faulted points at an Associate area's keypads, the Shared and Associate areas must share the same account number. The Scope of keypads assigned to Associate areas must include Shared areas.

Force Arming a Shared Area
When the keypad displays [CHECK AREA], press the NEXT key until the Force Arm? prompt shows. 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 for the Shared area.

Viewing Shared Area Armed Status
To view a Shared area's armed state, use the [VIEW AREA STATUS] command. Users must have an authority level assigned to the Shared area.

Silencing alarms and troubles in Shared areas
Users can silence alarms and troubles in Shared areas from any keypad. Users must have an authority level assigned to the Shared area.

Access Control Readers assigned to Shared areas
If the entry area is armed and is a Shared area, the exit delay restarts and allows a user to walk to an Associate area and disarm. If the card reader assigned to the Shared area includes any Associate areas in the D## KP# Scope (in the ACCESS CONTROL section), both the Associate area and Shared area disarm when the card is presented.

Closing Reports for Shared Areas
For closing reports for Shared areas, users must have a valid authority level assigned for the Shared area.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Type

5.1.13 Two Man Rule?

Default: No
Selections:
Yes - to disarm the area, two different passcodes entered at the same keypad required.
No - entering one passcode disarms the area.

Notice!
SIA CP-01 requirement
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.

Use this parameter in an areas disarmed from All On using keypads with *Scope, page 114*. An alarm event occurs if entry delay ends before the user enters the second passcode.
If the area alarm bell is sounding, entering the first passcode silences the alarm. Entering the second passcode disarms the area.
If the second passcode is entered using a different keypad than the first passcode, the second keypad warns the user that the two man rule is running, and to enter both passcodes at the same keypad.

You can create a custom function that disarms 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, page 114* parameter for keypads in the affected areas to "Area Wide."
Do not set Two Man Rule to Yes in an area that has *Early Ambush?, page 102* 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

5.1.14 Early Ambush?

Default: No

Selections:
Yes - after the area is disarmed, a duress relay activates and sends a duress report if a second valid passcode entry does not occur within the Early Ambush timeframe.
No - single passcode entry with a valid authority level can disarm the area.

Notice!
SIA CP-01 requirement
To comply with SIA CP-01 False Alarm Reduction standard, set this parameter to No for all enabled areas. Refer to SIA CP-01 Verification for more information.

This parameter controls the disarming of an area without duress. A duress report is automatically sent if a second valid disarm passcode is not entered within the timeframe set in *Early Ambush Time, page 82*.
The first passcode entered disarms the area; the second passcode entered validates the disarm. The passcodes can be the same and can be entered from any 2 keypads in the area. You can configure a second ambush code using the *Second Ambush Code, page 82* parameter selections. This function only operates when you use passcode disarm.

Notice!
Two man rule enabled
Do not set Early Ambush to Yes in an area that also has *Two Man Rule?, page 101* set to Yes.

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

5.1.15 Fire and Gas Time

Default: 6

Selections: 0 to 90 (minutes)
Enter the length of time in minutes the fire bell activates for fire and gas alarm points. A setting of 0 minutes will persist output until restored.

Notice!
Check with AHJ
Check with the local Authority Having Jurisdiction (AHJ) to confirm the appropriate bell time for the installation.

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 a minimum of two minutes.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fire and Gas Time

5.1.16 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 - 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent.
- Temporal Code 3 - 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off.

Select the pattern this area uses for alarms on a fire point. Patterns repeat until Fire Time expires.
Patterns repeat 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.)

Notice!
Two points sharing output in alarm
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

5.1.17 Burg Time

Default: 6
Selections: 0 to 90 (minutes)
Enter the length of time in minutes the alarm bell activates for burglary alarm points. The setting of 0 minutes will persist output until restored.

Notice!
Check with AHJ
Check with the local Authority Having Jurisdiction (AHJ) to confirm the appropriate bell time for the installation.

Notice!
SIA CP-01
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 A# *Alarm Bell, page 135* output activates when the burglary alarm occurs. It shuts off when the Burg Time expires.
Set this parameter for a minimum of two minutes.

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

5.1.18 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 - 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent. Repeats until fire bell time expires.
- Temporal Code 3 - 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off. Repeats until bell time expires.

Select the bell pattern this area uses for alarms on non-fire points. Patterns repeat until Burg Time expires.

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

5.1.19 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 - 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent.
- Temporal Code 3 - 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off.
- Temporal Code 4 - 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.

Select the bell pattern this area uses for alarms on a gas point. Patterns repeat until Fire Time expires.

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

5.1.20 Single Ring

Default: No
Selections:
- Yes - after one alarm event, subsequent alarm events on non-fire points in the same area, during the same armed period, do not activate the bell output.
- No - the bell output activates for each alarm event.

Single Ring does not affect the keypad alarm tone, or prevent any reports.
Fire points are not affected and bell time restarts with each new alarm.
Silencing the bell resets Single Ring.

Notice!
Keyswitch does not clear Single Ring
If an alarm occurs on a 24-hour point while the area is disarmed, arming that area with a keyswitch does not reset Single Ring.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Single Ring

5.1.21 Bell Test

Default: No
Selections:
- Yes - as a bell test, activate the Alarm Bell output for two seconds after receiving the acknowledgement from the central station receiver for the closing report (or at the end of exit delay for control panels that do not send closing reports).
- No - Bell test is disabled.

Notice!
Bell Test for All On arming only
The Bell Test feature only works when the area is armed All On. The Bell Test feature does not work when the area is armed Part On.

Bell Test after closing report
For areas configured to send opening and closing reports, the alarm bell output activates for two seconds when the control panel receives the acknowledgment for a closing report from the central station receiver.
When this Bell Test parameter is set to Yes, do not configure the Area for restricted openings and closings, or opening and closing windows.

Bell test after exit delay
When this Bell Test parameter is set to Yes and the area is not configured to send opening and closing reports, the alarm bell output activates for two seconds when exit time expires.

Arming multiple areas at the same time
When arming more than one area at the same time (using the ARM ALL AREAS? function for example) the control panel simultaneously sends closing reports for each area to the central station receiver. The bell test occurs when the control panel receives the acknowledgement for each report.
If closing reports are not sent, and all areas have the same exit delay time, the Alarm Bell output activates for two seconds for each area, with a two-second pause between each.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Bell Test

5.1.22 Account O/C

Default: No
Selections:
- Yes - send opening and closing reports by account for this area.
- No - do not send opening and closing reports by account.

The control panel sends an account closing report when the last area in the account is closed (armed).
The control panel sends an account opening report 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. Account opening and closing reports do not contain area information.
Set this parameter the same for all areas in the account.
Confirm the Account Number is the same all areas included the account.
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, page 106* 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.

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

5.1.23 Area O/C

Default: Yes
Selections:
- Yes - include the area information in opening and closing reports for this area. Send reports for areas individually.
- No - no area opening and closing reports for this area.

When this parameter is set to Yes and the *Account O/C, page 105* parameter is set to No, opening and closing reports include area information. The control panel sends reports for individual areas.
If Acct O/C is set to Yes, the control panel sends an account closing report (no area information) when the last area with the same account number is armed. The control panels sends an account opening report (no area information) when the first area with the same account number is disarmed.
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, page 166* 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

5.1.24 Disable O/C in Window

Default: Yes
Selections:
- Yes - do not send opening and closing reports to the central station if the open or close event occurs inside an active window.
- No - send opening and closing reports to the central station even when the open or close event occurs inside a programmed window.

If this parameter is set to Yes and an open or close event occurs outside of a window, the control panel sends the opening or closing report with an early or late modifier. Refer to O/C Windows
If this parameter is set to No and an opening or closing event occurs outside of the appropriate window, the control panel does not include early or late modifiers with opening or closing reports.
Open and close events are always logged.

If you want to monitor all opening and closing activity, but want to use features provided by opening and closing windows, set this parameter to No, and program O/C windows.

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

5.1.25 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.

Regardless of *Force Arm/Bypass Max, page 96* or *Bypassable, page 211*, an unconditional force arm occurs resulting in faulted points being left out of the system. Refer to *Force Arm Returnable, page 211* or *Bypass Returnable, page 211* for details on returning these points to service.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Auto Close

5.1.26 Fail to Open

Default: No
Selections:
– Yes - the control panel sends a Fail to Open report if the area is not disarmed at the Open Window Stop time.
– No - Fail to Open reports are not sent for this area.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Fail To Open

5.1.27 Fail to Close

Default: No
Selections:
– Yes - the control panel sends a Fail to Close report if the area is not armed at the Close Window Stop time.
– No - Fail to Close reports are not sent for this area.

Opening and closing reports do not need to be programmed to send Fail to Close reports. An exit delay time must be programmed in *Exit Delay Time, page 97*.
If *Auto Close, page 107* is set to Yes, a report is sent because it occurs when the closing window stop time occurs.
If *Disable O/C in Window, page 106* is set to Yes, the 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

5.1.28 Latest Close Time

Default: Disabled
Selections:
– Disabled - feature is disabled for the area.

Use Latest Close Time with the *Extend Close, page 236* feature to limit the extension of the closing time for an area. For example if the Latest Close Time is set to 19:30, you can only extend the expected closing time to as late as 19:29.
If the Latest Close Time setting is set to a non-zero value, the time of day specified in the *Close Window Start, page 228* 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

5.1.29 Restricted O/C

Default: No
Selections:
– Yes - restrict opening and closing reports for this area
– No - do not restrict opening and closing reports for this area.

When set to Yes, opening reports are only sent when the area is disarmed after non-fire/gas alarm. Closing reports are only sent when the area is armed All On with faulted points.
The sequence of reports generated by a restricted closing: Was Force Armed, Forced Point, Forced Close, Closing Report.
If a passcode is not required for turning the system on, closing reports are always restricted when Restricted O/C is Yes. If a passcode is required for turning the system on, the user must also be assigned an *Authority Levels, page 166* with Restricted Open/Close = E (enabled) in order for O/C reports to be restricted.
Area O/C, page 106 must be set to Yes to generate restricted opening and closing reports.
Active Open/Close Windows do not prevent restricted opening and closing reports. 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

5.1.30 Part On O/C

Default: No
Selections:
– Yes - send opening and closing reports for Part On Instant and Part On Delay.
– No - do not send opening and closing reports for Part On Instant or Part On Delay.

Part On opening and closing reports are not suppressed by Open/Close Windows.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Part On O/C

5.1.31 Exit Delay Restart

Default: Yes
Selections:
Yes - enable Exit Delay Restart.
No - disable Exit Delay Restart.
The Exit Delay Restart feature restarts exit delay when an end-user reenters the premises before exit delay expires.
For example, a homeowner turns on (arms) their system, leaves and closes the door, then realizes they forgot to pick up the car keys. When they open the door to retrieve their keys, the control panel restarts exit delay, giving them plenty of time to turn the system off.

With this parameter is set to Yes, following these steps restarts exit delay (*Exit Delay Time, page 97*):

1. Turn the system All On or Part On.
2. Fault and restore a point (open and close a door) assigned to a Point Profile configured for the Point Type, Part On, and a delayed alarm Point Response (4, 5, 6, 7, or 8). (*Point Profiles, page 188*, *Point Type, page 190*, *Point Response, page 195*)
3. With exit delay still running, fault any point (open a door) assigned to a Point Profile configured for the Point Type, Part On, and a delayed alarm Point Response (4, 5, 6, 7, or 8). Exit Delay restarts.

Notice!
Exit delay restarts only one time
Exit Delay can only be restarted one time. Faulting the same point again, or faulting a different point in the restarted exit delay does not restart the delay a second time.

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

5.1.32 All On - No Exit

Default: Yes
Selections:
Yes - the control panel switches arming from All On Delay to Part On Delay if no Part On Delay points are faulted and restored during the Exit Delay Time.
No - the control panel does not switch arming.
The final armed state is reported and displayed at the keypads.
When arming from a keyfob or SKED, the panel ignores this option.

Notice!
Area Auto Re-Arm (Part on Delay) use
Set the All On - No Exit parameter to No for an area when using Auto Re-Arm.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > All On - No Exit

5.1.33 Exit Delay Warning

Default: No
Selections:
– Yes - pulse the alarm output on and off every two seconds for the last 10 seconds of Exit Delay.
– No - do not pulse the alarm output during Exit Delay

Notice!
SIA CP-01 Requirement
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

5.1.34 Entry Delay Warning

Default: No

Selections:
- Yes - pulse the alarm output on and off every two seconds for the last 10 seconds of Entry Delay.
- No - do not pulse the alarm output during Entry Delay

Notice!
SIA CP-01 Requirement
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 > Entry Delay Warning

5.1.35 Area Re-Arm Time

Default: 00:00
Selections: 00:00 (disabled) thru 23:59
This parameter sets the length of time (HH:MM) that a disarmed area delays until it rearms to All On Delay.
For example if Area Re-Arm Time is set to four hours (04:00) and the area is disarmed (turned off) at 1:30 pm, it rearms to All On Delay at 5:30 pm. Any points not ready to arm (faulted) are force armed.

Notice!
Force Arm / Bypass Max is ignored when re-arming
All points not ready to arm (faulted) are force armed when the area re-arms at the end of Area Re-Arm Time.

The area automatically re-arms at 11:59 pm regardless of when the Area Re-Arm timer started.
For example, if the Area Re-Arm timer is set to 4 hours (04:00) and the area is disarmed (turned off) at 10:30 pm, the area rearms to All On Delay at 11:59 pm (1 hour and 29 minutes after disarm).
Users can use Extend Close time from a system keypad to extend an active Area Re-arm delay
(On/Off Menu > Extend Close time).

Notice!
Configuring Closing Window and Area Re-Arm Time may cause unexpected Area behavior.
When both a Closing Window and Area Re-Arm Time are configured for the same area,
the Closing Window is running simultaneously with the Area Re-arm timer,
and a user uses the Extend Close time from a system keypad,
the control panel extends only the Closing Window, not the Area Re-Arm Time.

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

5.1.36 Environmental Time

Default: 6
Selections: 0 to 90 (minutes)
Enter the length of time in minutes the alarm bell activates for Environmental alarm points. The setting of 0 minutes will persist output until restored.

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

5.1.37 Environmental 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 - 10 seconds audible + 5 seconds silent + 10 seconds audible + 5 seconds silent.
- Temporal Code 3 - 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 0.5 seconds Off, 0.5 seconds On, 1.5 seconds Off.
- Temporal Code 4 - 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.

Select the bell pattern this area uses for alarms on an Environmental Point Type. Patterns repeat until Environmental Time expires.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options >Environmental Pattern

5.2 Area Arming Text

The B6512 supports up to 6 areas.

5.2.1 Area name text

Default: Area # (# = the Area number)
Selections: Up to 32 characters of text, numbers, spaces, and symbols
Enter an Area name for display at keypads.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area Name Text

5.2.2 Account is On text

Default: Blank
Selection: Enter up to 32 characters.
Enter the text to display at the keypad for each area as required.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Account is On Text

5.2.3 Area # is On text

Default: Blank
Selection: Enter up to 32 characters.
Enter the text to display at the keypad for each area as required.

RPS Menu Location
Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # is On Text

5.2.4 Area # is not Ready text

Default: Blank

Selection: Enter up to 32 characters.

Enter the text to display at the keypad when the area is not ready to arm.

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # Not Ready Text

5.2.5 Area # is Off text

Default: Blank

Selection: Enter up to 32 characters.

Enter the text to display at the keypad when the area is Off (disarmed).

RPS Menu Location

Area Wide Parameters > Area/Bell Parameters, Open/Close Options > Area Arming Text > Area # is Off Text

6 Keypads

6.1 Keypad Assignments

The B6512 control panel supports SDI2 Keypads 1 to 12.
The B940W keypad is a subset of the B942 keypad. Because of the keypad hardware differences, some RPS programming features are not applicable for the B940W keypad:

Programming feature	B940W	B942
Proximity Reader	Not applicable	Available
Onboard Inputs and Outputs	Not applicable	Available
Presence Detector	Not applicable	Available
Power Requirements	Standby 250 mA Alarm 365 mA	Proximity reader disabled: – Standby 200 mA, Alarm 300 mA Proximity reader enabled: – Standby 300 mA, Alarm 400 mA

6.1.1 Keypad Name (first language)

Default: Keypad#
Selections: Up to 32 characters
Enter up to 32 characters of text, numbers and symbols to describe the keypad.
Keypads display the first 20 characters. When more than 20 characters are used, the keypad scrolls the complete text across the display one time. To scroll the text again, press [ESC].
Spaces count as text and are included in the 32 character limit.

RPS Menu Location
Keypads > Keypad Assignments > Keypad Name

6.1.2 Keypad Name (second language)

Default: blank
Selections: Up to 32 characters
Enter up to 32 characters of text, numbers and symbols to describe the keypad.
Keypads display the first 20 characters. When more than 20 characters are used, the keypad scrolls the complete text across the display one time. To scroll the text again, press [ESC].
Spaces count as text and are included in the 32 character limit.

RPS Menu Location
Keypads > Keypad Assignments > Keypad Name (second language)

6.1.3 Keypad Type

Default:
– Address 1 = B92x Two-line Keypad
– All other addresses = No Keypad Installed
Selections:
– No keypad installed
– B91x Basic Keypad
– B92x Two-line Keypad
– B93x ATM Style Keypad

– B94x Touch Screen Keypad

Select keypad type for the keypad connected to the control panel at this address. The Keypad Type is auto-configured when the keypad is first installed.

RPS Menu Location

Keypads > Keypad Assignments > Keypad Type

6.1.4 Area Assignment

Default: 1: Area 1 (for all KP addresses)

Selections:

– B6512: 1 to 6

Select an area to assign to the keypad.

If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location

Keypads > Keypad Assignments > Area Assignment

6.1.5 Keypad Language

Default: First Language, follow User language

Selections:

– First Language, follow User Language
– First Language, ignore User Language
– Second Language, follow User language
– Second Language, ignore User language

Select a language for the keypad.

RPS Menu Location

Keypads > Keypad Assignments > Keypad Language

6.1.6 Scope

Default:

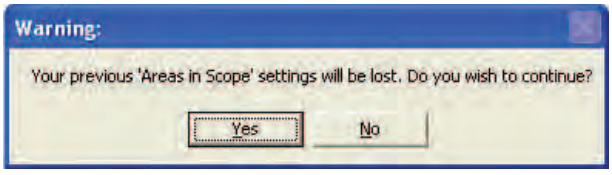
– Address 1: Panel Wide
– All other Addresses: Area Wide

Selections:

– Area Wide - keypad only shows information and arming/disarming functions for the area it is assigned to.
– Account Wide - keypad can show information, and arming/disarming functions for areas that share the same account number. Typically used for Associate area type.
– Panel Wide - A panel wide keypad can view information and perform arming and disarming functions for all areas in the control panel. Typically used with a Master area.
– Custom - for a custom scope, you select the Areas in Scope.

Scope determines which areas are can be viewed from the keypad, are included when arming from the keypad, and the keypad can move to.

Whenever Custom is selected, RPS shows the following warning dialog:



If you click Yes, Areas In Scope is reset to the default.

If you click No, no changes are made.

Further information
Account Number, page 96
Area Type, page 100
Areas in Scope, page 115

RPS Menu Location
Keypads > Keypad Assignments > Scope

6.1.7 Areas in Scope

Default:
– Address 1: All
– All other Addresses: Area1

Selections:
– click Area # to select or un-select an area
– click Set All to select all areas.
– click Clear All to clear all areas (select none)

Double click to view and select areas.
Click the areas to include in the Custom scope for this keypad.

Further information
Scope, page 114

RPS Menu Location
Keypads > Keypad Assignments > Areas in Scope

6.1.8 Passcode Follows Scope?

Default: Yes

Selections:
– Yes - when area the keypad is assigned to is armed, entering a passcode disarms the area and any other areas included in the scope of the keypad. When the area is disarmed, the area and any other areas included in the scope of the keypad are armed.
– No - entering a passcode only arms or disarms the area the keypad is assigned to.

Passcode Follows Scope applies to passcode arming only. It does apply to the arming functions in the Function List.
Users must be assigned to an Authority Level with Arm by Passcode and Disarm by Passcode enabled.

Further information
Scope, page 114
Area, page 185
Arm by Passcode, page 178
Disarm by Passcode, page 178

RPS Menu Location
Keypads > Keypad Assignments > Passcode Follows Scope

6.1.9 Enter Key Output

Default: 0: Unassigned

Selections:
– 1-3, 9-96 - assigns output for Passcode Enter Function, Cycle Output.
– 0 - no output assigned to Passcode Enter Function, Cycle Output.

When the *Passcode Enter Function, page 116* is set to Cycle Output, and a user enters their passcode and presses [Enter], the Enter Key Output activates for 10 seconds. Two events are added to the panel log: Output ### Set with User ID and, Output ### Reset without User ID.

Notice!
Do not share Enter Key Output with other output functions
The output you assign in this Enter Key Output parameter must not be assigned to any other output function. Erroneous output operation can result.

You can use the Passcode Enter Function, Cycle Door and the Enter Key Output for a low-level access control strike on a door. It does not shunt a point.

Further information
Passcode Enter Function, page 116
If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location
Keypads > Keypad Assignments > Enter Key Output

6.1.10 Passcode Enter Function

Default: Arm/Disarm
Selections:

- Arm/Disarm - when the current area is disarmed, entering passcode + [ENTER] starts All On Delay arming for all areas within the users scope. If the current area is armed, then all areas in the users scope are disarmed.
- Cycle Door - entering passcode + [ENTER] cycles the door controller programmed in Assign Door # for the Strike Time duration, and then executes arming functions (disarm for example) and custom functions per the user's authority level.
- Cycle Output - entering passcode + [ENTER] key activates the Enter Key Output for 10 seconds.
- Auto Re-Arm - if the area assigned to the keypad is armed All On Delay, entering passcode + [ENTER] re-starts Exit Delay. When the area is disarmed, passcode + [ENTER] does not arm.
- Login Only - passcode + [ENTER] key logs in the user. Dual authentication does not apply.
- Login/Disarm - Passcode + [ENTER] key logs in the user and disarms all areas in the users scope. Dual Authentication does not apply.

Entry of a passcode with authority in the current area always silences alarms and troubles.

Notice!
Area Auto Re-Arm (Part on Delay) use
Set the All On - No Exit parameter to No for an area when using Auto Re-Arm.

When a Passcode Enter Function is unable to be executed due to configuration conflicts, then the control panel performs the Arm/Disarm function regardless of setting.
The Service Passcode (User ID 0) cannot be used for Passcode Enter Functions.
Outputs used for the Cycle Output function must not be shared with any other point, sensor reset, control panel, or bell functions. Sharing can cause errors in output operation.

Notice!
Dual Authentication not compatible with Auto Re-Arm
If the Dual Authentication parameter is set to Yes, do not set this Passcode Enter Function parameter to Auto Re-arm.

Notice!
SIA CP-01 Requirement
To comply with SIA CP-01 False Alarm Reduction, keep this parameter at its default setting.

RPS Menu Location
Keypads > Keypad Assignments > Passcode Enter Function

6.1.11 Dual Authentication

Default: No
Selections:
- Yes - users must enter a passcode **and** present a credential (card or token) at a door reader or B94X Touch Screen Keypad, for arming, disarming, and password protected user functions.
- No - users enter a passcode **or** present a credential (card or token) at a B94X Touch Screen Keypad.

Notice!
Dual Authentication not compatible with Auto Re-Arm
If this Dual Authentication parameter is set to Yes, do not set the Passcode Enter Function parameter to Auto Re-arm.

RPS Menu Location
Keypads > Keypad Assignments > Dual Authentication

6.1.12 Dual Authentication Duration

Default: 20 Seconds
Selections: 10, 15, 20, 25, 30, 35, 40, 45 seconds
When Dual Authentication is enabled, users must enter a passcode **and** present a credential (card or token) within this duration.

RPS Menu Location
Keypads > Keypad Assignments > Dual Authentication Duration

6.1.13 Assign Door

Default: 0: No Door
Selections:
- No Door - No door controller assigned to the keypad.
- Door 1 to Door 4 - assign a door controller to the keypad by selecting its number.

Select the door controller (Door ##) the keypad uses for adding cards/tokens and the Close Door display.
When this Assign Door parameter is set to No Door, NOT READY appears at the keypad when users attempt to add a user. Until a door controller is assigned, users cannot use the keypad to assign cards/tokens with the Add/Edit User command.
When a door controller is not assigned to the keypad, users can control doors using the DOOR CONTROL functions.

Setting Assign Door to No Door disables:
- the Cycle Door option of Passcode Enter Function,
- the Add Card option of the Add/Change User command,
- Dual Authentication.

If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location
Keypads > Keypad Assignments > Assign Door

6.1.14 Trouble Tone

Default:
- Yes - B9512G/B8512G control panels

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

Panel wide trouble tones include power, phone, SDI bus, and SDI2 bus. They do not include point troubles, or buzz on fault.

RPS Menu Location
Keypads > Keypad Assignments > Trouble Tone

6.1.15 Entry Tone

Default: Yes

Selections:
- Yes - This keypad sounds the entry tone during entry delay.
- No - This keypad does not sound the entry tone.

Faulting a delay point in the area scope of the keypad starts entry delay.
To suppress entry tone per point, set the Points > Point Profile > *Entry Tone Off, page 206* parameter to Yes.
Set this parameter to Yes for UL installations.

RPS Menu Location
Keypads > Keypad Assignments > Entry Tone

6.1.16 Exit Tone

Default: Yes

Selections:
- Yes - This keypad sounds the exit tone during exit delay.
- No - This keypad does not sound the exit tone.

Arming from a keypad that has a scope to arm the area starts exit delay.
To suppress exit tone by area, set the Area Wide Parameters > Exit Tone parameter to No.

RPS Menu Location
Keypads > Keypad Assignments > Exit Tone

6.1.17 Arm Area Warning Tone

Default: Yes

Selections:
- Yes - at the start of a closing window the keypad sounds a tone and shows a warning.
- No - this keypad does not sound a tone or show a warning.

RPS Menu Location
Keypads > Keypad Assignments > Arm Area Warning Tone

6.1.18 Close Door Warning Tone

Default: Yes
Selections:
– Yes - when a door is held open past the Shunt Time, the keypad sounds a warning tone and shows Close Door.
– No - this keypad does not activate a warning tone or show Close Door.

The Access / Door / *Extend Time, page 247* parameter for the door assigned to the keypad in the *Assign Door, page 117* parameter must be set to a value greater than zero.

RPS Menu Location
Keypads > Keypad Assignments > Close Door Warning Tone

6.1.19 Idle Scroll Lock

Default: No
Selections:
– Yes - when the keypad is idle, it does not auto-scroll text for silenced alarm or trouble events.
– No - allow text to auto-scroll.

RPS Menu Location
Keypads > Keypad Assignments > Idle Scroll Lock

6.1.20 Function Lock

Default: No
Selections:
– Yes - after pressing the Bypass, Menu, or Shortcuts key, users must enter a passcode to continue.
– No - a passcode is not required to continue.

When this parameter is set to Yes, users are prompted to enter a passcode after pressing the Bypass, Menu, or Shortcuts key. The items programmed in the function list for this 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.

Notice!
D1256 Fire keypads and D1257 Fire annunciators
If using a D1256 Fire keypad and D1257 Fire annunciator, Bosch recommends that you do not set the Function Lock parameter to Yes. The Yes setting will prompt the operator to enter a passcode. The D1256 Fire keypad has no keys for entering this passcode.

RPS Menu Location
Keypads > Keypad Assignments > Function Lock

6.1.21 Abort Display

Default: Yes
Selections:

– Yes - this keypad shows ALARM NOT SENT if a burglar alarm is aborted before an alarm report is sent.
– No - this keypad does not show ALARM NOT SENT.

RPS Menu Location
Keypads > Keypad Assignments > Abort Display

6.1.22 Cancel Display

Default: Yes
Selections:
– Yes - this keypad shows CANCELLED ALARM when a burglar alarm is canceled.
– No - this keypad does not show CANCELLED ALARM.

When this parameter is set to Yes, the Panel Wide / Miscellaneous / *Cancel Reports, page 80* parameter must be set to Yes.

RPS Menu Location
Keypads > Keypad Assignments > Cancel Display.

6.1.23 Nightlight Enable

Default: No
Selections:
– Yes - the keypad display backlight and the key backlight are on at the minimum level when the keypad is idle.
– No - the keypad display backlight and the key backlight are off when the keypad is idle.

When this parameter is set to Yes, users can turn the nightlight feature on or off at the keypad.

RPS Menu Location
Keypads > Keypad Assignments > Nightlight Enable

6.1.24 Nightlight Brightness

Default: 2
Selections:
– 0 - Nightlight off
– 1 to 6 - the higher the number, the brighter the nightlight.

This parameter sets the brightness level for the keypad Nightlight feature.

RPS Menu Location
Keypads > Keypad Assignments > Nightlight Brightness

6.1.25 Silence Keypress Tone

Default: No
Selections:
– Yes - keypad is silent when keys are pressed.
– No - keypad sounds the keypress tone when a user presses a key.

When this parameter is set to No, users cannot turn the keypress tone off.
When this parameter is set to Yes, users cannot turn the keypress tone on.

RPS Menu Location
Keypads > Keypad Assignments > Silence Keypress Tone

6.1.26 Show Date and Time

Default: No

Selections:
- Yes - the keypad shows the date and time.
- No - the keypad does not show the date and time.

RPS Menu Location
Keypads > Keypad Assignments > Show Date and Time

6.1.27 Keypad Volume
Default: 7
Selections: 0 to 7
0 is the lowest volume.
7 is the highest volume.
High priority tones, alarm tone for example, always sound at maximum volume.

RPS Menu Location
Keypads > Keypad Assignments > Keypad Volume

6.1.28 Keypad Brightness
Default: 6
Selections: 0 to 6
0 - the keypad display is dimmest.
6 - the keypad display is brightest.
Users can set the keypad brightness at the keypad.

RPS Menu Location
Keypads > Keypad Assignments > Keypad Brightness

6.1.29 Disable Presence Sensor
Default: No
Selections:
- Yes - disable presence sensor
- No - when the presence sensor detects motion near the keypad, the keypad brightens a dimmed display.

Only B94x Touch Screen keypads have the presence sensor feature.

RPS Menu Location
Keypads > Keypad Assignments > Disable Presence Sensor

6.1.30 Disable Token Reader
Default: Yes

Selections:
- Yes - disable Token Reader.
- No - enable Token Reader.

Only the B94x Touch screen keypads have the Token Reader feature.
Disabling the token reader reduces power consumption.

RPS Menu Location
Keypads > Keypad Assignments > Disable Token Reader

6.1.31 Enable Tamper Switch
Default: No
Selections:
- Yes - enable the Tamper Switch.

– No - disable the Tamper Switch.

This parameter only applies to SDI keypads and the B915 keypad.

RPS Menu Location

Keypads > Keypad Assignments > Enable Tamper Switch

6.1.32 Feature Button Option

Default: Language Selection

Selections:

– Language Selection - users press the button to toggle between the control panel's first and second languages.

– Event Memory - users press the button to quickly access and view Event Memory.

This parameter configures the feature button in the upper left corner of the B94x Touch Screen Keypad.

RPS Menu Location

Keypads > SDI2 Keypad Assignments > Feature Button Option

6.1.33 Supervision

Default: Yes

Selections:

– Yes - this keypad address is supervised. Only connect one SDI keypad set to this address.

– No - this keypad address is not supervised. You can connect more than one SDI keypad set to this address.

This parameter applies to SDI keypads only. SDI2 keypads are always supervised.

The *Keypad Type, page 113* parameter must be set to an SDI keypad.

When this parameter is set to Yes and a problem occurs with the keypad or the SDI bus, the control panel creates a TROUBLE SDI ## event.

SDI D125xRB Fire Keypads are supervised, even when this parameter is set to no.

SDI keypads sharing the same address setting display the same text and sound the same tones when keys are pressed on any one of them.

SDI Trouble events are always for Area 1, Account 1 no matter which area the SDI device is assigned.

RPS Menu Location

Keypads > Keypad Assignments > Supervision

6.1.34 Passcode [Esc] Option

Default:

– No for Keypad #1 (SDI2 keypad) and Yes for all others.

Selections:

– Yes - entering a passcode followed by [Esc] silences active alarms. If acknowledged alarms are showing, entering passcode plus [Esc] clears the display.

– No - entering a passcode and then pressing the [Esc] key erases the last digit of the passcode. Continuing to press [ESC] erases digits one at a time. When no digits are left pressing [ESC] exits the task.

Notice!
PANEL WIDE PARAMETERS > Miscellaneous > Passcode Length must be set to Disabled
When the PANEL WIDE PARAMETERS > Miscellaneous > Passcode Length parameter is set to 3 Digits, 4 Digits, 5 Digits, or 6 Digits, this Passcode [Esc] Option is disabled, even when it is set to Yes.
When this Passcode [Esc] Option is set to Yes, you must set the PANEL WIDE PARAMETERS > Miscellaneous > Passcode Length parameter to Disabled.

Notice!
UL 985 requirements for Household Fire Warning System Units
Configure this setting to Yes (require a passcode) to comply with UL 985 requirements.

RPS Menu Location
Keypads > Keypad Assignments > Passcode [Esc] Option

6.2 Global Keypad Settings

6.2.1 A-key Response

Default: No Response
Selections:
- No Response - invalid key tone sounds.
- Manual Fire Alarm - creates a fire alarm event when users hold the A-key and the 1-key at the same time for 2 seconds, or when users push CMD then 7 (Command 7).
- Custom Function - executes the selected custom function when users hold the A-key for 2 seconds. Use the A-key Custom Function parameter to select the custom function. The Custom Function selection does not apply to B942 touch screen keypads.

When this parameter is set to Manual Fire Alarm an alarm event occurs each time the user presses the appropriate keys, whether or not previous alarms are cleared from the display.

Notice!
Manual Fire Alarm includes CMD-7, set the Authority Level / User Command 7 parameter to "E"
Setting A-key response to Manual Fire Alarm also configures CMD-7 (Command 7) for manual fire alarm. When users push CMD + 7.

RPS Menu Location
Keypads > Global Keypad Settings > A-key Response.

Refer to
- *RPS Menu Location, page 206*

6.2.2 A-key Custom Function

Default: Disabled
Selections:
- B6512G: Disabled, Function 128 to Function 133

Select the custom function that runs when users hold the A-key for 2 seconds.
The A-key Response parameter must be set to Custom Function.

RPS Menu Location
Keypads > Global Keypad Settings > A-key Custom Function

6.2.3 B-key Response

Default: No Response
Selections:
- No Response - invalid key tone sounds.
- Manual Medical Alarm, no alarm output - creates a medical alarm event when users hold the B-key and the 4-key at the same time for 2 seconds. The alarm output is **not** activated for the medical alarm event.
- Manual Medical Alarm, with alarm output - creates a medical alarm event when users hold the B-key and the 4-key at the same time for 2 seconds. The alarm output is activated for the medical alarm event.
- Custom Function - executes the selected custom function when users hold the B-key for 2 seconds. Use the B-key Custom Function parameter to select the custom function. The Custom Function selection does not apply to B942 touch screen keypads.

When this parameter is set to Manual Medical Alarm, no alarm output or to Manual Medical Alarm, with output, an alarm event occurs each time the user presses the appropriate keys, whether or not previous alarms are cleared from the display.

RPS Menu Location
Keypads > Global Keypad Settings > B Key Response

6.2.4 B-key Custom Function

Default: Disabled
Selections:
- B6512G: Disabled, Function 128 to Function 133

Select the custom function that runs when users hold the B-key for 2 seconds.
The B-key Response parameter must be set to Custom Function.

RPS Menu Location
Keypads > Global Keypad Settings > B Key Custom Function

6.2.5 C-key Response

Default: No Response
Selections:
- No Response - invalid key tone sounds.
- Manual Panic Alarm, invisible and silent alarm output - creates a panic alarm event when users hold the C-key and the 7-key at the same time for 2 seconds, or when users push CMD then 9 (Command 9).
  The event does **not** show in the keypad display. The **silent** alarm output activates.
- Manual Panic Alarm, visible with alarm output - creates a panic alarm event when users hold the C-key and the 7-key at the same time for 2 seconds, or when users push CMD then 9 (Command 9).
  The event shows in the keypad display. The alarm output activates.
- Custom Function - executes the selected custom function when users hold the C-key for 2 seconds. Use the C-key Custom Function parameter to select the custom function. The Custom Function selection does not apply to B942 touch screen keypads.

When this parameter is set to Manual Panic Alarm, invisible and silent alarm output, or to Manual Panic Alarm, visible with alarm output, an alarm event occurs each time the user presses the appropriate keys, whether or not previous alarms are cleared from the display.

RPS Menu Location
Keypads > Global Keypad Settings > C-key Response

6.2.6 C-key Custom Function

Default: Disabled
Selections:
– B6512G: Disabled, Function 128 to Function 133

Select the custom function that runs when users hold the C-key for 2 seconds.
The C-key Response parameter must be set to Custom Function.

RPS Menu Location
Keypads > Global Keypad Settings > C Key Custom Function

6.2.7 Manual Silent Alarm Audible on Comm Trouble

Default: No
Selections:
– Yes - the Alarm Bell activates when a silent alarm report fails to reach central station after two attempts.
– No - the Alarm Bell does **not** activate when a silent alarm report fails to reach central station.

This parameter applies when a keypad C-key, or a RADION keyfob panic, creates silent alarm events.
When set to Yes, the Alarm Bell output activates for Burg Bell time minus the time for two attempts to send the silent alarm report. The Burg Bell timer starts when the silent alarm event is created.

RPS Menu Location
Keypads > Global Keypad Settings > Manual Silent Alarm Audible on Comm Trouble

6.2.8 Card Type

Default: 26 bit
Selections:
26 bit
35 bit Corporate 1000 (B9612G, B8612G, B6612 only)
37 bit

Default *Site Code, page 153* for card types
26 bit: default site code is 255
35 bit Corporate 1000: default site code is 4095 (B9612G, B8612G, B6612 only)
37 bit no site code: default site code is blank. The site code is not configurable (Site Code parameter is grayed out).
37 bit with site code: default site code is 65535 (B9612G, B8612G, B6612 only)

RPS Menu Location
Keypads > Global Keypad Settings > Card Type

6.2.9 Comm Trouble Options

Default: Comm Troubles are Audible and Visible

Selections:
- Comm Troubles are Silent and Invisible - communication trouble events do not show at the keypads and do not sound the trouble tone.
- Comm Troubles are Audible and Visible - communication trouble events show at the keypads and sound the trouble tone.

Notice!
Enable trouble tone for each keypad
Use the *Trouble Tone, page 118* parameter in Keypad assignments to enable panel wide trouble tones (including the Comm Trouble) for individual keypads.

RPS Menu Location
Keypads > Global Keypad Settings > Comm Trouble Sound Options

6.3 Global Wireless Keyfob

6.3.1 Keyfob Function A Custom Function

Default: Disabled
Selections:
- B6512G: Disabled, Function 128 to Function 133

Select the custom function that runs when users push the Function A button on RADION keyfobs.

RPS Menu Location
Keypads > Global Wireless Keyfob > Keyfob Function A Custom Function

6.3.2 Keyfob Function B Custom Function

Default: Disabled
Selections:
- B6512G: Disabled, Function 128 to Function 133

Select the custom function that runs when users push the Function B button on RADION keyfobs.

RPS Menu Location
Keypads > Global Wireless Keyfob > Keyfob Function B Custom Function

6.3.3 Keyfob Panic Options

Default: Panic response disabled
Selections:
- Panic response disabled - the control panel ignores panic button presses from all keyfobs.
- Audible panic response enabled - when users press a panic button on a keyfob, the control panel creates a keyfob panic alarm event, shows the alarm and sounds the alarm tone at keypads, and activates the Alarm Bell output.
- Silent panic response enabled - when users press a panic button on a keyfob, the control panel creates a keyfob silent alarm event and activates the silent alarm output. Keypads remain silent and do not show the alarm.

When the Alarm Bell output is active, silencing the alarm creates a Cancel event.
When the silent panic response is active, acknowledging the alarm creates a Cancel event.
The Alarm Abort feature does not apply to keyfob panic alarm or keyfob silent alarm events.

The control panel does not create restoral events for keyfob panic alarm events or keyfob silent alarm events.

RPS Menu Location
Keypads > Wireless keyfob > keyfob Panic Options

7 Custom Functions

Use the parameters in this section to configure custom functions.
The B6512 supports 6 custom functions.

7.1 Custom Function Text (first language)

Default: Function ###
Selection: Up to 18 characters of text, numbers, spaces, and symbols.
Enter text to identify the custom function at keypads.

RPS Menu Location
Custom Function > Custom Function Text

7.2 Custom Function Text (second language)

Default: (blank)
Selection: Up to 18 characters of text, numbers, spaces, and symbols.
Enter text to identify the custom function at keypads.

RPS Menu Location
Custom Function > Custom Function Text (second language)

7.3 Functions

Default: Not in Use

Selections: Refer to the list below.
Use these Function parameters (Function 1 to Function 6) to assign up to six functions to a custom function.
Double click in the Function 1 (to Function 6) field to show the function selection dialog box. Some functions require you to configure one or two parameters. For example, if you select the Disarm function, you select which areas to disarm in Parameter 1.

Notice!
When a Custom Function initiates, assigned functions run in order, 1 to 6
The control panel runs the functions assigned to a custom function consecutively. The panel starts functions immediately after starting the previous function. It does not wait for the previous function to finish.
Use the Delay function selection to create a delay between the start of two functions. Parameter 1 configures the length of the delay (1 to 90 seconds).
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 Parameter 1 set to greater than 30 seconds, and set Function 3 to "Toggle Output".

Notice!

Special Force Arm / Bypass Max rules for arming with Custom Functions

When a Custom Function includes an arming function (All On Delay, All On Instant, Part On Instant, Part On Delay) special rules for the *Force Arm/Bypass Max, page 96* limit for faulted points apply.

If a user activates the Custom Function from a keypad using a shortcut or function key, from an RF Keyfob, or by presenting their credential (card or token) to a reader or keypad, and the Custom Function requires a passcode (*Custom Function, page 165* = P), then the control panel enforces the Force Arm / Bypass Max limit for faulted points. If the number of faulted points exceeds the Force / Arm Bypass Max limit, the function fails The control panel does not arm the Area. There is no indication at keypads for the failed function. The control panel includes the user number in the arming event (history log and report).

If a user activates a Custom Function from a keypad using a shortcut or function key, from an RF Keyfob, or by presenting their credential (card or token) to a reader or keypad, and the Custom Function does not require a passcode (*Custom Function, page 165* = E), then the control panel enforces the Force Arm / Bypass Max limit for faulted points. If the number of faulted points exceeds the Force / Arm Bypass Max limit, the function fails The control panel does not arm the Area. There is no indication at keypads for the failed function. The control panel does not include the user number in the arming event (history log and report).

If a custom function is activated by a Sked, point, or automation, the control panel does *not* enforce the Force Arm / Bypass Max limit for faulted points. The control panel arms all faulted points, even if the Force Arm / Bypass Max limit is exceeded.

FUNCTION:

Not In Use - This function is disabled and no functions after this will be performed.
All On Delay, page 235
All On Instant, page 236
Part On Delay, page 236
Part On Instant, page 236
Disarm, page 236
Extend Close, page 236
Bypass a Point, page 236
Unbypass a Point, page 236
Unbypass All Points, page 236
Reset Sensors, page 130
Turn Output On, page 237
Turn Output Off, page 237
Toggle Output, page 237
One-Shot Output, page 130
Reset All Outputs, page 237
Delay, page 130
Cycle Door, page 130
Unlock Door, page 237
Lock Door, page 237
Secure Door, page 237
Access Ctrl Level, page 237
Access Granted Events, page 237
Access Denied Events, page 238

Answer RPS, page 130
Contact RPS, page 238
Contact RPS User Port, page 238
Send Status Report, page 238
Send Test Report, page 238
Send Test on Off Normal, page 240
Go to Area, page 131
Watch On, page 240
Watch Off, page 240
Show Date & Time, page 240
Sound Watch Tone, page 240
Set Keypad Volume, page 241
Set Keypad Brightness, page 241
Trouble Silence, page 131
Alarm Silence, page 131

RPS Menu Location
Custom Function > Function 1-6

7.4 Custom Function descriptions

The functions in this section are not activated by a Sked and are not available as a Sked *Function, page 233*.

7.4.1 Reset Sensors

This function emulates the keypad shortcut Reset Sensors. When activated, this function activates the area-wide-output Reset Sensors for 5 seconds. This function de-activates the alarm output for areas selected in Parameter 1 for five seconds.

7.4.2 One-Shot Output

This function is not available as a keypad shortcut function and is only available as a custom function. The function activates the output selected in Parameter 1 for the number of seconds selected in Parameter 2.

7.4.3 Delay

Use this function to create a configurable delay (0 to 90 seconds) between, or before functions. Parameter 1 configures the delay.

7.4.4 Cycle Door

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

7.4.5 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.

7.4.6 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 #.

7.4.7 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 #.

7.4.8 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 #.

8 Shortcut Menu

8.1 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: Brightness (SDI2) / Bright (SDI)
- Shortcut Menu Item 7: Volume (SDI2) / Dim (SDI)
- Shortcut Menu Item 8: View Log
- Shortcut Menu Item 9-32: Disabled Item

Selections:

Use this parameter to assign 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 (first language), page 128*.

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
Disabled Item	Invisible Walk Test	Set Panel Time
All On Delay	Send Test Report	Show Date/Time
All On Instant	Display Revisions	Change Skeds
All On Select Area	RPS Answer	Brightness (SDI2)
Part On Delay	RPS via Network	Volume (SDI2)
Part On Instant	RPS via Network, Change	Keypad Nightlight
Part On Select Area	Port	Silence Key Tone
Off	RPS via Phone	View Event Memory
Off Select Area	Go to Area	Delete Event Memory
Extend Close	Update Firmware	View Log
Bypass a Point	View Service Bypassed	A Key Alarm (Fire)
Unbypass a Point	Cycle Door	B Key Alarm (Medical)
View Area Status	Unlock Door	C Key Alarm (Silent/Panic)
View Point Status	Lock Door	Function ### (128 to 133)
Send Status Report	Secure Door	
Reset Sensors	Change Passcode	
Change Output State	Add User	
Fire Walk Test	Edit User	
Intrusion Walk Test	Delete User	
Service Walk Test	Change Watch Mode	
	Set Panel Date	

RPS Menu Location

Shortcut Menu > Function

Not In Use - This function is disabled and no functions after this will be performed.
All On Delay, page 235
All On Instant, page 236
Part On Delay, page 236
Part On Instant, page 236
Disarm, page 236
Extend Close, page 236
Bypass a Point, page 236
Unbypass a Point, page 236
Unbypass All Points, page 236
Turn Output On, page 237
Turn Output Off, page 237
Toggle Output, page 237
Reset All Outputs, page 237
Unlock Door, page 237
Lock Door, page 237
Secure Door, page 237
Access Ctrl Level, page 237
Access Granted Events, page 237
Access Denied Events, page 238
Contact RPS, page 238
Contact RPS User Port, page 238
Send Status Report, page 238
Send Test Report, page 238
Send Test on Off Normal, page 240
Watch On, page 240
Watch Off, page 240
Show Date & Time, page 240
Sound Watch Tone, page 240
Set Keypad Volume, page 241
Set Keypad Brightness, page 241
Execute Custom Function, page 241

8.2 Set/Clear all

Default: Set/Clear All
Selections: Address 1-12
Use this parameter to enable or disable functions at all addresses.

RPS Menu Location
Shortcut Menu > Set/Clear All

8.3 Address

Default: Yes (Shortcut Menu 1 to 8)
Selections:
– Yes - include in the menu for keypads set to this address.
– No - do not include in the menu.

RPS Menu Location
Shortcut Menu > Address # (1 to 32)

9 Outputs

Panel outputs are programmed to operate based on a range of available Triggers for one specific area or the entire system (Panel Wide). Outputs provide dry contact (normally open/closed) outputs for LED annunciation and other applications including wet (12vdc on/off) voltage outputs for basic alarm system functions (such as Bell output, Reset Sensors, etc.). In some cases, functional sources for outputs may include Unassigned, also known as a virtual output, or an IP Camera.

Output Types

- Panel Wide Outputs 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 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 are 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 for the B6512 control panel can control as many as 64 dry contact form "C" outputs when up to 8 optional B308 OctoOutput modules are installed. These outputs are used for Area Output, Panel Wide Output, and Individual Point Fault Outputs.

Output Profiles

Output Profiles allow advanced output programming and operations by providing a way for an output to operate based more than one output type; including Panel Wide, Area specific Triggers, point states and more. Once an Output Profile is programmed and saved, it can be reused and assigned to multiple outputs enabling quick output programming.

You can create Output Profiles that define the way an output operates when specific events occur. Output Profiles provide a way to assign and use consistent output effects across a panel, area, or point.

Output Profiles contain 1 or 2 Triggers that may include Scope, Scope Filter, Pattern, Delay and Duration settings to produce a specific output effect.

Notice!

Firmware Requirement

Output Profiles require Panel Firmware 3.10 or newer to operate. When assigned, all other programming using the same output is ignored.

Output Reports

Output reports are stored in the control panel memory log.

Controlling Outputs

Outputs can be activated depending upon events that exist with the control panel. Also, outputs can be controlled by the user using the [CHG OUTPUT?] function, Output On/Output Off Skeds, and RPS.

Output C is always powered ON. Assigning any other output deactivates Output C, so that 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 Output C provides a path to common. Output C turns off the common connection during sensor reset. Check the 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 must be manually reset with the Change Output function:

Fail To Close	Force Armed
Duress	Log % Full

9.1 Area Wide Outputs

9.1.1 Alarm Bell

Default: 1

Selections:

– 0 (disabled), 1 to 96

This output activates when an intrusion point assigned to the area goes into alarm. It also activates for (non-fire) keypad and keyfob alarms that are configured to sound the Alarm Bell.

The output activates for the time entered in the *Burg Time, page 103* parameter. The out follows the cadence set in the *Burg Pattern, page 104* parameter. The *Silent Alarm, page 138* parameter must be set to No in order for the bell to ring upon alarm.

Notice!

SIA CP-01 requirement

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.

RPS Menu Location

Outputs > Area Wide Outputs > Alarm Bell

9.1.2 Fire Bell

Default: 1

Selections:

– 0 (disabled), 1 to 96

This Fire Bell output activates when a fire point assigned to the area goes into alarm. It also activates for keypad fire alarms and fire drills.
The output activates for the time entered in the *Fire and Gas Time, page 102* parameter. The output follows the cadence set in the Fire Pattern parameter.

Notice!
UL 864 requirement
To comply with UL 864 requirements for Commercial Fire Systems, program this parameter with a relay.

RPS Menu Location
Outputs > Area Wide Outputs > Fire Bell

9.1.3 Reset Sensors

Default: 3 (OUTPUT C)
Selections:
– 0 (disabled), 1 to 96

The output you enter here activates for five seconds when users start the Reset Sensors user function or during a Fire Walk test.
When assigning an output to Reset Sensors for two or more areas, you must set the parameters below. Failure to do so can cause a trouble event for *Resettable, page 214* points.
– Keypad *Scope, page 114* must include all the areas that share the output.
– Users must have authority for *Reset Sensor(s), page 175* in all the areas that share the output.
– *Restart Time, page 98* must be set to the same number of seconds for all the areas that share the output.

RPS Menu Location
Outputs > Area Wide outputs > Reset Sensors

9.1.4 Fail to Close/Part On Armed

Default: 0 (disabled).
Selections:
– 0 (disabled), 1 to 96

When the Part On Output parameter is set to no, this Fail to Close / Part On Armed output activates when the closing window for the area expires. It remains activated until midnight, until another closing window starts, or the control panel is reset.
When the Part On Output parameter is set to Yes, this Fail to Close / Part On Armed output activates when all areas assigned to the same output are armed Part On Instant or Part On Delayed.
Refer to *Part On Output, page 85*.
Use the *Early Area Armed Output, page 85* parameter to select if a Part On Delayed output activates at the beginning of exit delay, or at the end of exit delay. The default is that the output activates at the end of exit delay.

RPS Menu Location
Outputs > Area Wide Outputs > Fail to Close/Part On

9.1.5 Force Armed

Default: 0 (disabled)

Selections:

– 0 (disabled), 1 to 96

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.

RPS Menu Location

Outputs > Area Wide Outputs > Force Armed

9.1.6 Watch Mode

Default: 0 (disabled)

Selections:

– 0 (disabled), 1 to 96

This output activates when a Watch Point is faulted when Watch Mode is enabled and the area is disarmed.
Watch Points are active when the Point Response is blank (no response). The Point Type must be 24 Hour, Part On, or Interior.

RPS Menu Location

Outputs > Area Wide Outputs > Watch Mode

9.1.7 Area Armed

Default: 0 (disabled)

Selections:

– 0 (disabled), 1 to 96

The output activates when the the area is All On (armed).
If multiple areas use the same output, the output activates when all areas are armed. It deactivates when the first area disarms.
The output remains activated until the area is Off (disarmed). The area does not deactivate during the entry delay time.
Use the *Early Area Armed Output, page 85* parameter to select if the Area Armed output activates at the beginning of exit delay, or at the end of exit delay. The default is that the output activates at the end of exit delay.

RPS Menu Location

Outputs > Area Wide Outputs > Area Armed

9.1.8 Area Off

Default: 0 (disabled)

Selections:

– 0 (disabled), 1 to 96

The output entered here activates when the area goes from All On (either delay or instant) to Part On or Off (disarmed).
When the area goes from Part On or Off to All On, the output de-activates.
If the same output is used for more than one area, when all the areas are All On, the output is de-activated. When the first area goes to Off (disarmed) or Part On, the output activates

When the *Early Area Armed Output, page 85* parameter is set to No, this Area Off output does not activate until the end of exit delay. When the Early Area Armed Output parameter is set to Yes, the Area Off Output de-activates as soon as exit delay starts and the area is armed All On.

RPS Menu Location
Outputs > Area Wide Outputs > Area Off

9.1.9 Area Fault

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates whenever a Part On, Interior or Interior Follower point is faulted. The output stays activated until all perimeter and interior points in the area are not faulted. You can use the Area Fault output to show that the area is not ready to arm.

RPS Menu Location
Outputs > Area Wide Outputs > Area Fault

9.1.10 Duress Output

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when a user creates a duress event at a keypad that is assigned to the area.
The output activates steady for the time entered in the *Burg Time, page 103* parameter. The *Burg Pattern, page 104* parameter has no effect this output.
The *Duress Enable, page 99* parameter must be set to Yes.

RPS Menu Location
Outputs > Area Wide Outputs > Duress Output

9.1.11 Part On Fault

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when a Part On point assigned to the area is faulted. The output activates regardless of the areas armed state (All On, Part On, or Off).
This output provides a steady output until all Part On points in the area are not faulted.

RPS Menu Location
Outputs > Area Wide Outputs > Part On Fault

9.1.12 Silent Alarm

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when a point assigned to a Point Profile with the Silent Bell parameter set to Yes goes into alarm.
Use this output for panic/hold up applications.

RPS Menu Location
Outputs > Area Wide Outputs > Silent Alarm

9.1.13 Gas Bell

Default: 1
Selections:
– 0 (disabled), 1 to 96

This Gas Bell output activates when a gas point assigned to the area goes into alarm.
The output activates for the time entered in the *Fire and Gas Time, page 102* parameter. The output follows the cadence set in the *Gas Pattern, page 104* parameter.

RPS Menu Location
Outputs > Area Wide Outputs > Gas Bell

9.1.14 Environmental Bell

Default: 0
Selections:
– 0 (disabled), 1 to 3, 9 to 96
The output activates for the time entered in the *Environmental Time, page 110* parameter.
The output follows the cadence set in the *Environmental Pattern, page 111* parameter.

RPS Menu Location
Outputs > Area Wide Outputs > Environmental Bell

9.2 Panel Wide Outputs

9.2.1 AC Failure

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when the control panel makes an AC Fail event. The output de-activates when the control panel creates an AC Restoral event.
The control panel waits the time entered in the *AC Fail Time, page 74* parameter to create the AC Fail and AC Restoral events.

RPS Menu Location
Outputs > Panel Wide Outputs > AC Failure

9.2.2 Battery Trouble

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96
The output activates when battery voltage falls below 12.1 VDC, or when the battery is in a missing condition. The output resets when battery power is restored.

RPS Menu Location
Outputs > Panel Wide Outputs > Battery Trouble

9.2.3 Phone Fail

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when the control panel makes a phone line fail event. The output automatically resets when the phone line restores.
The control panel waits the time entered in the *Phone Supervision Time, page 32* parameter before it makes phone line fail events and phone line restoral events.

RPS Menu Location
Outputs > Panel Wide Outputs > Phone Fail

9.2.4 Comm Fail

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

When there is a Comm Fail event for any Route Group the output activates. The output resets when a report from the Route Group is sent to the central station receiver successfully.
To learn more about Comm Fail events refer to *Communicator, overview, page 63*.

RPS Menu Location
Outputs > Panel Wide Outputs > Comm Fail

9.2.5 Log % Full

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when the log reaches the percentage of its capacity set in the Log % Full parameter. The output de-activates when RPS resets the log pointer.
Refer to *Log % Full, page 76*.

Further information
See Get History for more information.

RPS Menu Location
Outputs > control panel Wide Outputs > Log % Full (Outputs)

9.2.6 Summary Fire

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any fire point in the system goes into alarm. The output de-activates when all fire points in the system return to normal, and all fire alarm events are cleared from keypad displays.

Notice!
This Summary Fire output only functions as described when the *Fire and Gas Summary Sustain, page 82* parameter is set to No.

Notice!
Do not assign more than one function to the output assigned to this Summary Fire function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Fire

9.2.7 Summary Alarm

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any non-fire or non-gas point goes into alarm. The output de-activates when all non-fire and non-gas points return to normal, all non-fire and non-gas alarms are silenced, and the alarm events are cleared from keypad displays.
This output does not activate for invisible points.

Notice!
Do not assign more than one function to the output associated with this Summary Alarm function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Alarm

9.2.8 Summary Fire Trouble

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any fire point in the system goes into trouble. The output de-activates when all fire points in the system return to normal, and all fire trouble events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Fire Trouble

9.2.9 Summary Supervisory Fire

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any fire supervisory point in the system goes into alarm. The output de-activates when all fire supervisory points in the system return to normal, and all fire supervisory alarm events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Supervisory Fire

9.2.10 Summary Trouble

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any non-fire or non-gas point goes into a trouble condition. The output de-activates when all non-fire and non-gas points in the system return to normal, and all non-fire and non-gas trouble events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Trouble

9.2.11 Summary Supervisory Burg

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any non-fire/non-gas supervisory point in the system goes into alarm. The output de-activates when all non-fire/non-gas supervisory points in the system return to normal, and all non-fire/non-gas supervisory alarm events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Supervisory Burg

9.2.12 Summary Gas Output

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96

The output activates when any gas point in the system goes into alarm. The output de-activates when all gas points in the system return to normal, and all gas alarm events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Gas Output

9.2.13 Summary Gas Supervisory Output

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96
The output activates when any gas supervisory point in the system goes into alarm. The output de-activates when all gas supervisory points in the system return to normal, and all gas supervisory alarm events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Gas Supervisory Output

9.2.14 Summary Gas Trouble Output

Default: 0 (disabled)
Selections:
– 0 (disabled), 1 to 96
The output activates when any gas point in the system goes into trouble. The output de-activates when all gas points in the system return to normal, and all gas trouble events are cleared from keypad displays.

Notice!
Do not assign more than one function to the output assigned to this summary function.

RPS Menu Location
Outputs > Panel Wide Outputs > Summary Gas Trouble Output

9.3 Output Assignments

9.3.1 Output Source

Default:
– Output A(1): On-board A
– Output B(2): On-board B
– Output C(3): On-board C

– All other Outputs: Unassigned

Selections:

– On-board
– Unassigned
– Octo-output
– Keypad
– IP Camera
– Aux Power Supply

Use this parameter to assign output numbers to output sources (physical devices). Selections that are grayed out are not available.

B308 Octo-output Modules have output number boundaries starting at Output 11.

For IP cameras, use *Camera Inputs-Outputs, page 44* to assist in assignment of panel points and panel outputs.

Use of IP Camera as Output Source is limited

Control panels can be configured to initiate communications to IP cameras using up to 4 Panel output assignments per IP Camera. The panel outputs available are specific for each IP camera.

For example, for “Camera 1”, you can assign Panel Outputs 11-18. For “Camera 2”, you can assign Outputs 21-28, for “Camera 4”, you can assign Outputs 41-48 and so on.

IP Camera as an Output Source is not available for Outputs 19 to 20, 29 to 30, 39 to 40, 49 to 50, 69 to 96.

Aux Power Supply output source support

Aux Power Supply is supported on these panel outputs:

– B6512: Outputs 17 to18, 27 to 28, 37 to 38, 47 to 48

RPS Menu Location

Outputs > Output Assignments > Output Source

Refer to

– *Camera Inputs-Outputs, page 44*
– *B308 Octo-output Module switch settings, page 270*

9.3.2 Output Text (First Language)

Default: Output #

Selections: Up to 32 alphanumeric characters

Enter a description of the output in the first language. Installers, service personnel, and users see this description.

RPS Menu Location

Outputs > Output Assignments > Output Text

9.3.3 Output Text (Second Language)

Default: Blank

Selections: Up to 32 alphanumeric characters

Enter a description of the output in the second language. Installers, service personnel, and users see this description.

RPS Menu Location

Outputs > Output Assignments > Output Text-Second Language

9.3.4 Output Profile

Default: Unassigned
Selections:
– Up to 20 profiles
Select the Output Profile to assign to an output. The output will operate exclusively according to the Output Profile programming. When an Output Profile is assigned to an output, the Trigger and behavior settings in the Output Profile override any other output parameter settings.
– Use an Output Profile to assign an advanced Output Behavior to 1 or multiple outputs.

Manual control (on/off) of outputs
Outputs based on Output Profiles can be turned on manually (by keypad or remotely) and will remain on.
Manually turn off outputs to return to automatic operation.

Further information
Panel Wide Outputs, page 139
Area Wide Outputs, page 135
Points, page 183
Point Profiles, page 188

RPS Menu Location
Outputs > Output Assignments > Output Profile

9.3.5 Hide From User

Default: No
Selections:
– Yes - keypads, RSC mobile app, SDK automation interfaces (such as Mode 1, Mode 2, SDK, VMS), and the BSM mobile app cannot view or control the output.
– No - keypads, RSC mobile app, SDK automation interfaces (such as Mode 1, Mode 2, SDK, VMS), and the BSM mobile app can view or control the output.
Use this parameter to disable the viewing or controlling of outputs from keypads, RSC, SDK integration interfaces, and the BSM mobile application.

RPS Menu Location
Outputs > Output Assignments > Hide from User

9.4 Output Profiles

9.4.1 Profile Name

Default: Output Profiles 1-13 have varied preset defaults, which are shown in the table. Output Profiles 14 and higher are disabled without any preset defaults.
Selections: Up to 32 alphanumeric characters
Use this parameter to name the Output Profile.
Output Profiles contain 1 or 2 Triggers that may include Scope, Scope Filter, Pattern, Delay and Duration settings to produce a specific output effect.

Output Profile defaults for profiles 1-13

Output Profile	Profile Name	Trigger 1	Scope 1	Scope 1 Filter	Pattern	Duration
1	Burg, Fire, Gas Alarm	Output Active	Output	1 - Output A (1)	On Steady	Follows Trigger
2	Reset Sensors	Output Active	Output	3 - Output C (3)	On Steady	Follows Trigger
3	Burg Alarm	Burglary Alarm	Panel Wide	0	On Steady	Until Off
4	Fire Alarm	Fire Alarm	Panel Wide	0	Half Second Pulses	Until Off
5	Fail To Close	Fail To Close	Panel Wide	0	On Steady	Follows Trigger
6	Part On Armed	Part on armed	Panel Wide	0	On Steady	Follows Trigger
7	Watch Active	Watch active	Panel Wide	0	On Steady	Follows Trigger
8	All On Armed	All on armed	Panel Wide	0	On Steady	Follows Trigger
9	Area Disarmed	Area disarmed	Panel Wide	0	On Steady	Follows Trigger
10	Area Fault	Area Fault	Panel Wide	0	On Steady	Follows Trigger
11	Gas Alarm	Gas Alarm	Panel Wide	0	Temporal Code 4	Until Off
12	Burg Supervisory (Monitor Delay)	Burglary Supervisory	Panel Wide	0	On Steady	Until Off
13	Entry / Exit Delay	Entry / Exit delay	Panel Wide	0	Half Second Pulses	Follows Trigger

Notice!
Firmware Requirement
Output Profiles require Panel Firmware 3.10 or newer to operate. When assigned, all other programming using the same output is ignored.

RPS Menu Location
Outputs > Output Profiles > Profile Name

9.4.2 Output Behavior

Behavior name:

– Output Behavior [A]

You can program an Output Profile with a different Output Behavior. An Output Behavior allows the combination of up to 2 Triggers (the same or different Output Type) to generate specific output effects. An Output Behavior effect is a Delay, Duration, and Pattern. Each selected Trigger must occur to satisfy the Output Profile conditions. Once satisfied, any output assigned to this profile will activate and operate per the Profile Pattern, Delay and Duration.

RPS Menu Location

Outputs > Output Profiles > Output Behavior

9.4.3 Trigger

Default: Disabled

Selections: Events, states or other parameter that produce an output effect. For example, a Fire Alarm, Burglary Alarm or Point.

Use this parameter to select the type of event that must occur to cause an output effect. You can define up to 2 Triggers for the Output Behavior. The selected Trigger will control the Scope and Scope Filter selections that are available.

Notice!

Configured Triggers Activate Output

Each programmed Trigger is required to satisfy the Output Profile conditions and activate an output.

RPS Menu Location

Outputs > Output Profiles > Trigger

Further information

The following events, states and parameters are available to use individually or in combination when configuring Triggers:

Fire Alarm *Fire Bell, page 135*

Gas Alarm *Gas Bell, page 139*

Burglary Alarm *Alarm Bell, page 135*

Burglary Supervisory *Summary Supervisory Burg, page 142*

Entry / Exit delay *Entry Delay, page 206* / *Exit Delay Time, page 97*

Area Fault *Area Fault, page 138*

All on armed - activates when an area is armed in an All On state.

Part on armed - activates at the end of the closing window when an output is set for *Fail to Open, page 107* and the area is not armed.

Area disarmed *Area Off, page 137*

Fail to Close *Fail to Close, page 107*

Watch active *Watch Mode, page 137*

Point Active - activates (assigned output turns on) when the configured point is faulted, open or shorted. You can assign any valid point number. *Source, page 183*

Output Active *Output, page 185*

SKED Activated Function - activates when the configured SKED runs at its scheduled day and time. *Function, page 233*

Custom Function Activated - activates (assigned output turns on) when a custom function that is configured in the *Scope Filter, page 148* for the Trigger runs at the panel. *Functions, page 128*
Ethernet Line Faulted - activates (assigned output turns on) when the panel has a trouble displayed for the on-board Ethernet connection. *On Board Ethernet (IP) Communicator, page 34*
AC Failure *AC Failure, page 139*
Battery Trouble *Battery Trouble, page 139*
Communication Fail *Comm Fail, page 140*
System Fault - activated when the panel has a general system fault, such as a missing device, missing keypad, or an SDI bus fault.
Area ready - activates when all of the Part On, Interior or Interior Follower points that are assigned to an area are normal. The output turns off if any of the Part On, Interior or Interior Follower points that are assigned to an area are faulted.

9.4.4 Scope

Default: Panel Wide

Selections:

- Panel Wide - panel or system effect
- Area Wide - area effect
- Point - point or zone effect
- Output - output effect
- Sked - Sked effect
- Custom Function - Custom Function effect

Use this parameter to select the focus of the Trigger. The selected Scope controls which Scope Filter options are available for selection.

Further information

The following parameters are available when configuring Scope and Scope Filter:
Panel Wide Parameters, page 31
Area / Bell Parameters, Open / Close Options, page 95
Points, page 183
Panel Wide Outputs, page 139
Area Wide Outputs, page 135
Functions, page 128
Sked Function descriptions, page 235

RPS Menu Location

Outputs > Output Profiles > Scope

9.4.5 Scope Filter

Default: 0

Selections are filtered automatically by the Scope parameter selection (Panel Wide, Area Wide, Point, Output, Sked, Custom Function). Actual selection strings are dynamic based on Panel programming:

- Panel Area and name
- Panel Point and name
- Output and name
- Sked and name
- Custom Function and name

Use this parameter to further focus the Trigger to a subset of the Scope. For example, Area 1 or Custom Function 2.

RPS Menu Location
Outputs > Output Profiles > Scope Filter

Further information
The following parameters are available when configuring Scope and Scope Filter:
Panel Wide Parameters, page 31
Area / Bell Parameters, Open / Close Options, page 95
Points, page 183
Panel Wide Outputs, page 139
Area Wide Outputs, page 135
Functions, page 128
Sked Function descriptions, page 235

9.4.6 Pattern

Default: Off
Selections:
- Off - none.
- On Steady - steady output.
- Half Second Pulse - pulsed march time. 60 beats per minute repeating at an even tempo (0.5 seconds on, 0.5 seconds off).
- One Second Pulse - pulsed march time. 30 beats per minute played once at an even tempo (1 second on, 1 second off).
- Two Second Pulse - pulsed march time. 15 beats per minute played once at an even tempo (2 seconds on, 2 seconds off).
- Temporal Code 3 - repeating sequence (0.5 seconds on, 0.5 seconds off, 0.5 seconds on, 0.5 seconds off, 0.5 seconds on, 1.5 seconds off).
- Temporal Code 4 - repeating sequence (100ms on, 100ms off, 100ms on, 100ms off, 100ms on, 100ms off, 100ms on, 5 seconds off). Zonex outputs (0.5 seconds on, 0.5 seconds off, 0.5 seconds on, 0.5 seconds off, 0.5 seconds on, 0.5 seconds off, 0.5 seconds on, 5 seconds off).
- California March - repeating sequence (10 seconds on, 5 seconds off).

Use this parameter to select the output effect pattern.

RPS Menu Location
Outputs > Output Profiles > Pattern

9.4.7 Delay

Default: 00:00:00
Selections (00:00:00, 00:00:05 - 02:00:00):
- hh - hours
- mm - minutes
- ss - seconds

Use this parameter to specify the length of time to wait (5 seconds to 2 hours) after a Trigger occurs before activating the output.
If Trigger 1 or Trigger 2 in an Output Profile is set to Watch active, then the Delay parameter cannot be changed. The default Delay selection is shown grayed out (no change accepted).

RPS Menu Location
Outputs > Output Profiles > Delay

9.4.8 Duration

Default: Until Off
Selections:
- Until Off - persists until the silence function is initiated.
- Timed - persists from 5 seconds up to 2 hours.
- Until Cleared - persists until the alarm and fault event are cleared. This selection cannot be silenced.
- Follows Trigger - persists until the Trigger event is cleared. This selection cannot be silenced.

Use this parameter to select how an assigned output persists after activating.

RPS Menu Location
Outputs > Output Profiles > Duration

10 User Configuration

10.1 User Assignments (passcodes)

10.1.1 User Name

Default:

– User 0: Installer

– All others: USER [user number]

Selections: Up to 32 characters (text, numbers, spaces, and symbols). Spaces before, after, and within the name are treated as text and are included in the 32 character limit.

Enter the user name to show at keypads. The user name is included in reports sent to the central station receiver in the Modem4 reporting format.

If the user name is longer than 20 characters, keypads scroll the full name one time and then show the first twenty characters. To scroll the name again, press [ESC].

RPS Menu Location

User Configuration > User Assignments > User Name

10.1.2 Passcode

Default:

– User 0: 123

– User 1: 123456

– All others: Blank

Selections: 0 to 9

Enter a 3 to 6 digit passcode.

The *Passcode Length, page 83* parameter sets the passcode length. When it is set to 3, 4, 5, or 6 digits, passcode length is fixed for all passcodes. Users do not need to press the Enter key after entering their passcode.

When the Passcode Length parameter is set to Disabled, passcode length is not fixed for all passcodes. Individual passcodes can be 3 to 6 digits in length. Users must press the Enter key after entering their passcode.

RPS will not let you enter a passcode that could conflict with a duress passcode. You cannot enter a passcode within a range of 2 of existing passcodes. For example, if 654327 is an existing passcode, you can not enter 654325, 654326, 654328, or 654329. RPS enforces this rule even if duress is disabled.

Installer Passcode

User 0 (Installer) cannot be added or edited at a keypad. When a user other than User 0 tries to delete the passcode for User 0, the keypad displays NOT IN USE.

RPS Menu Location

User Configuration > User Assignments (Passcodes) > Passcode

10.1.3 Mobile Access

Default: No

Selections:

– Yes (allow this user system access with the mobile app)

– No (prohibit this user from system access with the mobile app)

When this parameter is set to Yes, this user can control their security system with a mobile device using the RSC (Remote Security Control) and BSM (Bosch Security Manager) mobile apps.

RPS Menu Location
User Configuration > User Assignments > Remote Access

10.1.4 User Group

Default: 0: Unassigned
This selection means a group is not assigned to the user record and User Group Windows or Group Level Area Authorities are not applied.
Selections:
B6512 Groups:
– 0: Unassigned, User Group 1- User Group 6
Use this parameter to make a group of users whose credentials (passcode, access card or token, and RF keyfob) are enabled and disabled by a User Group Window. Assign a User Group to restrict passcode authority and re-apply any group area authorities. You can assign a user group to multiple user group windows.
The 0: Unassigned selection means a user group is not restricted to any SKED and is not granted any group authority level.
– You can override any group-applied authority to an area by editing the specific Area Assignment for a user.
– Changes to Area Authorities using User Assignments > User Group will not automatically update existing User Assignments. You can re-apply the group defined Area Authorities by re-assigning the User Group to a user.
Enter the User Group number into the Schedules > User Group Windows *>User Group, page 230* parameter for any enabled window.
For example, if User Group 1 is assigned to a window running from 8:00 AM (start time) to 4:00 PM (stop time), the users in the group can use their credentials only between 8:00 AM and 4:00 PM.

RPS Menu Location
User Configuration > User Assignments (Passcodes) > User Group

10.1.5 Area Authorities

Default:
– User 0: All Area #'s (A1-An) Authority Level = 15
– User 1:
  – Area #1 (A1) Authority Level = 1
  – All other Area #'s Authority Level = 0
– All Other User #'s:
  – All Areas (A1-An): Authority Level = 0
B6512 Areas (A1-A6):
– 0: No Authority, Auth Level 1- Auth Level 14

Notice!
Installer User 0 (Authority Level 15) reserved
Authority Level 15 cannot be set for user group area authority.

When setting up a new user, make sure to assign an authority level for at least one area to the user. The Area Authorities parameter defaults to 0 (zero) for new users, which means the user has no authority in the area indicated. Authority level 15 is reserved for User 0, Installer.

Use the Area columns (A1-An) to set the users Authority level to each individual Area. Alternatively, you can apply Group level Area Authorities across multiple Areas using User Groups.
When using Group defined Area Authorities to apply User Authorities across multiple Areas (A1-An):

- You can override any group-applied authority to an area by editing the specific Area Assignment for a user.
- Changes to Area Authorities using User Assignments > User Group will not automatically update existing User Assignments. Group defined Area Authorities are only applied to user records by re-assigning the User Group to a user.

Refer to User Configuration > *Authority Levels, page 166* and User Configuration > User Groups > *Area Authorities, page 155* in RPS to view settings for each authority level.

RPS Menu Location
User Configuration > User Assignments > Area Authorities

10.1.6 Site Code

Default (per card type)**:**

- 26 bit card type: 255
- 32 bit MIFARE Classic card type: blank (read only)
- 35 bit Corporate 1000 card type: 4095
- 37 bit no site code card type: blank
- 37 bit with site code card type: 65535

Selections (per card type)**:**

- 26 bit card type: 0 to 254, 255 = disabled
- 32 bit MIFARE Classic card type: blank
- 35 bit Corporate 1000 card type: 0 to 4094, 4095 = disabled
- 37 bit no site code card type: blank
- 37 bit with site code card type: 0 to 65534, 65535 = disabled

For the 37 bit no site code card type, the Site Code parameter is grayed out.
For 26 bit card type and 37 bit with site code card type, enter the site code (facility code) as shown on the card or token packaging.
For 35 bit card type, enter the site code at the keypad (User Menu) or by swiping the card at the reader/keypad. After the card is swiped, the site code is associated with the user, and is available in User Configuration > User Assignment (passcodes) parameters.
To get the site code using RPS, add the card or token into the system at the premises using a reader and keypad (MENU 42). Then connect to the panel with RPS and receive the panel account.
When you delete a card (or delete the card data) RPS automatically sets the Site Code to the default (255 for the 26 bit card type, 4095 for the 35 bit card type, 65535 for the 37 bit with site code card type).

RPS Menu Location
User Configuration > User Assignments > Site Code

10.1.7 Card Data

Default: blank

Selections:

- 26 bit card type: 0 to 65534, blank
- 32 bit MIFARE Classic card type: 0 to 4294967294, blank
- 35 bit Corporate 1000 card type: 0 to 1048574, blank

– 37 bit no site code card type: 0 to 34359738366, blank
– 37 bit with site code card type: 0 to 524286, blank

Enter the card data printed on the card or token.

For the **26 bit, 35 bit** and **37 bit with site code** *Card Type, page 251*, enter the *Site Code, page 153* before you enter Card Data. The maximum values are reserved and will reset the Site Code and Card Data parameters to the default values if a higher value is entered. For example, entering 65535 for the 26 bit card type will reset the Site Code and the Card Data selection back to the default values.

RPS Menu Location
User Configuration > User Assignments > Card Data

10.1.8 Inovonics Keyfob RFID (B820)

Default: N/A
Selections: 0 - 99999999
To assign an Inovonics Keyfob to this user, enter the RFID (Radio Frequency device Identification number). The number is printed on the keyfob.
Inovonics keyfobs are not supervised when assigned to a user.
You can also auto-learn the RFID locally using the SDI2 bus RF receiver and a system keypad.
Setting the RFID to 0 to disables the user's keyfob.

Notice!
RFID updates go to SDI2 bus RF receiver after you disconnect RPS
When you send RFID updates from RPS to the control panel, the control panel does not download the RFIDs to the SDI2 bus RF receiver until you disconnect RPS.

RPS Menu Location
User Configuration > User Assignments > Keyfob RFID (B820 Inovonics Wireless)

10.1.9 RADION Keyfob RFID (B810)

Default: 0
Selections: 0, 11 - 167772156
To assign a RADION Keyfob to this user, enter the RFID (Radio Frequency device Identification number). The number is printed on the keyfob.
You can also auto-learn the RFID locally using the SDI2 bus RF receiver and a system keypad.
Setting the RFID to 0 to disables the user's keyfob.

Notice!
RFID updates go to SDI2 bus RF receiver after you disconnect RPS
When you send RFID updates from RPS to the control panel, the control panel does not download the RFIDs to the SDI2 bus RF receiver until you disconnect RPS.

RPS Menu Location
User Configuration > User Assignments > Keyfob RFID (B810 RADION Wireless)

10.1.10 Supervised

Default: No
Selections:

– Yes - the RADION keyfob assigned to this user is supervised.
– No - the RADION keyfob assigned to this user is not supervised.

When this parameter is set to Yes, the control panel creates a missing event when the keyfob is out of range of the RADION receiver for 4 hours.
Inovonics keyfobs are not supervised.

RPS Menu Location
User Configuration > User Assignments > Supervised

10.1.11 User language

Default: 1: [first language]
Selections:
– 1: [first language]
– 2: [second language]

Select the language the user sees at keypads configured to show the user language.
First language and second language are set during panel account setup in the Panel Data View.

RPS Menu Location
User Configuration > User Assignments (Passcodes) > User Language

10.2 User Groups

10.2.1 User Group Name

Default: Blank
Selections: Up to 32 characters (text, numbers, spaces, and symbols). Spaces before, after, and within the name are treated as text and are included in the 32 character limit.
Use this parameter to enter a name for the user group.

RPS Menu Location
User Configuration > User Groups > User Group Name

10.2.2 Area Authorities

Default:
– Not Overwrite

B6512 Areas (A1-A6):
– Not Overwrite, 0: No Authority, Auth Level 1- Auth Level 14

Notice!
Installer User 0 (Authority Level 15) reserved
Authority Level 15 cannot be set for user group area authority.

Use the Area columns (A1-An) to set one or many Area Authorities that you want to apply to a user record. Group Area Authorities will be applied to a user record each time the group is assigned to a user record in User Assignments.
– You can override any group-applied authority to an area by editing the specific Area Assignment for a user.
– Changes to Area Authorities using User Assignments > User Group will not automatically update existing User Assignments. You can re-apply the group defined Area Authorities by re-assigning the User Group to a user.

RPS Menu Location

User Configuration > User Groups

Refer to
– *User Group, page 152*

10.3 User (keypad) Functions

10.3.1 All On Delay

Default: P

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

This user function arms areas All On with entry delay and exit delay. All controlled points in the area are included.

RPS Menu Location

User Configuration > User Keypad Functions > All On Delay

10.3.2 All On Instant

Default: P

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

This user function arms areas All On with no entry delay and no exit delay. All controlled points in the area are included.

Notice!
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 > All On Instant

10.3.3 Part On Instant

Default: P

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

This user function arms areas Part On with no entry delay and no exit delay. Only Part On points in the area are included. Interior points are not included.

Notice!
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

10.3.4 Part On Delay

Default: P

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

This user function arms areas Part On with entry delay and exit delay. Only Part On points in the area are included. Interior points are not included.

RPS Menu Location

User Configuration > User Keypad Functions > Part On Delay

10.3.5 Watch Mode

Default: E

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

This user function toggles watch mode on and off.

When watch mode is on and a watch point is faulted, the keypads show the point text and sound the watch tone.

RPS Menu Location

User Configuration > User Keypad Functions > Watch Mode

10.3.6 View Area Status

Default: P

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

This user 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

10.3.7 View/Delete Event Memory

Default: E

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

This user function shows event memory. Event memory is deleted (cleared) when the area is armed.

RPS Menu Location
User Configuration > User Keypad Functions > View/Delete Event Memory

10.3.8 View Point Status

Default: E
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.
– Passcode (P) - Require a passcode to enable this function panel wide.

This user function shows the point text and the electrical state (normal, open, short, or missing) of each point assigned to the area.

RPS Menu Location
User Configuration > User Keypad Functions > View Point Status

10.3.9 Walk Test (all Non-Fire Burg Points)

Default: E
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.
– Passcode (P) - Require a passcode to enable this function panel wide.

The Walk Test user function allows users to test controlled points without sending alarm reports to the central station receiver.
At the start of the Walk Test, the Alarm Bell output activates for 2 seconds. As the user faults each controlled point, the keypads beep once.
Fire points, gas points, and 24 hour points cannot be tested using this Walk Test user function.

RPS Menu Location
User Configuration > User Keypad Functions > Walk Test (All Non-Fire Burg Points)

10.3.10 Walk Test All Fire Points

Default: P
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.
– Passcode (P) - Require a passcode to enable this function panel wide.

This parameter disables, enables without passcode required, or enables with passcode required, the Fire Walk Test user function.

Notice!
Fire walk test includes gas and environmental points
When you perform a Fire Walk Test, the security system tests any 24-hour points that are not invisible. The Fire Walk Test includes gas, environmental (water, high temp, low temp) and any uncontrolled visible points.

When a Fire Walk Test starts
– The control panels sends a FIRE WALK START report to the central station receiver.
– There is local alarm annunciation only, no alarm reports are sent to the central station receiver.
– The control panel is powered by the battery only.

- The *Fire Bell, page 135* output activates for 2 seconds for each fire point or gas point that is tested.
- All fire points and gas points with the *Resettable, page 214* parameter set to YES, automatically reset when tested. [SENSORS RESETTING] shows at keypads.
- The keypad shows the point text for each point as each it is tested, and an updated "points tested" count.
- The test ends after all points are tested or after 20 minutes of no activity. The control panel sends a FIRE WALK END report to the central station receiver.

If fire points or gas points are faulted when Fire Walk Test ends, the points are bypassed and the trouble tone sounds. The keypads show the bypassed points and the trouble condition.

When a Fire Drill starts

- The control panel sends a FIRE DRILL START report to the central station receiver.
- The *Fire Bell, page 135* output activates until a user ends the drill by silencing the Fire Bell.
- Fire points and gas points are active. An alarm on a fire point or gas point ends the drill. The control panel sends Fire alarm reports.

When the fire drill ends, the control panel sends a FIRE DRILL END report.

RPS Menu Location

User Configuration > User Keypad Functions > Walk Test All Fire Points

10.3.11 Send Report (Test/Status)

Default: E

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

This user function sends the same test report as the sked function.

If a point in any area is off normal (trouble not cleared from the keypad display), the control panel sends a test off-normal report instead of the test report.

If the Panel Wide Parameters > Report Routing > *Expand Test Report, page 33* parameter is set to Yes, the test report (or test off-normal report) is followed by a diagnostic report for each off-normal system status. Refer to Panel Wide Parameters > Report Routing > *Diagnostic Reports, page 59* for a list of reports included.

RPS Menu Location

User Configuration > User Keypad Functions > Send Report (Test/Status)

10.3.12 Door Control

Default: P

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

The users functions enabled by this parameter are: cycle door, unlock door, and secure door.

RPS Menu Location

User Configuration > User Keypad Functions > Door Control

10.3.13 Set Keypad Brightness / Volume / Keypress

Default: E

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

This function lets users adjust keypad brightness and volume, and set the keypress tone on or off.

For B942 keypads, users can set the night light and presence features.

RPS Menu Location

User Configuration > User Keypad Functions > Set Keypad Brightness/Volume/Keypress

10.3.14 Set/Show Date and Time

Default: P

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

This user 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

10.3.15 Change Passcode

Default: P

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

This user function allows a user to change their own passcode.

To allow a user to change the passcode for other users, refer to the *Add/Edit User, page 160* function.

RPS Menu Location

User Configuration > User Keypad Functions > Change Passcode

10.3.16 Add/Edit User

Default: P

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.
– 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.

Notice!

Add User command stops response to door control and RTE/REX requests

When the ADD USER command is running, credentials (cards or tokens) are not processed. There is no response to door control functions and RTE/REX requests. If there is heavy activity for a door, set the door to the Unlocked state before adding users.

RPS Menu Location
User Configuration > User Keypad Functions > Add/Edit User

10.3.17 Delete User

Default: P
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.
– 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

10.3.18 Extend Close

Default: P
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.
– Passcode (P) - Require a passcode to enable this function panel wide.
This function allows users to extend the closing window when the Close Early Begin time has passed and the closing window is active.

RPS Menu Location
User Configuration > User Keypad Functions > Extend Close

10.3.19 View Event Log

Default: E
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.
– 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

10.3.20 User Command 7

Default: P
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.
– Passcode (P) - Require a passcode to enable this function panel wide.
Pressing [CMD] then [7] causes a manual fire alarm response.
With B92x keypads, holding the [A] and [1] keys together also causes a manual fire alarm response.
To enable User Command 7 you must set the Keypads > Global Keypad Settings > A Key Response to Manual Fire Alarm.

RPS Menu Location
User Configuration > User Keypad Functions > User Command 7

10.3.21 User Command 9

Default: P

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

Pressing [CMD] then [9] causes a manual panic alarm response.
With B92x keypads, holding the [C] and [7] keys together, also causes a manual panic alarm response.
To enable User Command 9 you must set the Keypads > Global Keypad Settings > C Key Response to Manual Panic Alarm, invisible and silent alarm output, or to Manual Panic Alarm, visible with alarm output.

RPS Menu Location

User Configuration > User Keypad Functions > User Command 9

10.3.22 Bypass a Point

Default: P

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.
– 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

10.3.23 Unbypass a Point

Default: P

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.
– 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 where the function is entered are unbypassed.

RPS Menu Location

User Configuration > User Keypad Functions > Unbypass a Point

10.3.24 Reset Sensor(s)

Default: E

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

This function resets sensors in areas within the Scope of the keypad.

RPS Menu Location

User Configuration > User Keypad Functions > Reset Sensor(s)

10.3.25 Change Output(s)

Default: P

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

This function allows the user to manually set and reset outputs.

Manual control (on/off) of outputs

Outputs based on Output Profiles can be turned on manually (by keypad or remotely) and will remain on.

Manually turn off outputs to return to automatic operation.

RPS Menu Location

User Configuration > User Keypad Functions > Change Output(s)

10.3.26 Remote Program

Default: P

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

This user function starts remote programming sessions. If the user starts this function when the phone line shared with the control panel is ringing, the control panel seizes the phone line.

RPS Menu Location

User Configuration > User Keypad Functions > Remote Program

10.3.27 Go to area

Default: P

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

This function temporarily assigns the keypad to a different area.

Users are limited to functions enabled by their authority level for the area that the keypad is temporarily assigned to.

After 15 seconds of no user activity at the keypad, the keypad reverts back to it's assigned area.

RPS Menu Location

User Configuration > User Keypad Functions > Move to Area

10.3.28 Display Panel Type and Revision

Default: E

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

This user function shows the control panel type and firmware revision.

When the Area Name Text parameter is changed from the default, this function shows the default Area Name Text.

RPS Menu Location
User Configuration > User Keypad Functions > Display Panel Type and Revision

10.3.29 Service Walk All Points

Default: P

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

The Service Walk Test user function allows users to test all points that are assigned to a Source (the Source parameter is not set to Unassigned).
As the user faults each point, the keypads beep once.
Fire points, gas points, or 24-Hour points left faulted when exiting the Service Walk Test are bypassed. The trouble tone sounds at keypads.

RPS Menu Location
User Configuration > User Keypad Functions > Service Walk All Points

10.3.30 Change Skeds

Default: P

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

This function allows the user to edit the time a Sked executes, and if the Sked runs on holidays. Users can execute this function from any keypad assigned to an area where the user has authority.

RPS Menu Location
User Configuration > User Keypad Functions > Change Skeds

10.3.31 Walk Test All Invisible Burg Points

Default: P

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

The Walk Test Invisible user function allows users to test invisible points (the Invisible Point parameter set to Yes) without sending alarm reports to the central station receiver.
24-Hour points left faulted when exiting the Invisible Walk Test are bypassed. The trouble tone sounds at keypads.
Fire points and gas points cannot be tested using this Walk Test Invisible user function.

RPS Menu Location
User Configuration > User Keypad Functions > Walk Test All Invisible Burg Points

10.3.32 Silence Function

Default: E

Selections:

– Enable (E) - enable the Silence Function panel wide without requiring the user to enter a passcode to silence trouble tones at the keypads.
– Passcode (P) - enable the Silence Function panel wide and require the user to enter a passcode to silence trouble tones at the keypads after pressing the Silence key or Enter key.

Pressing the Silence key or the Enter key on a keypad stops the keypad from sounding trouble tones that have occurred due to trouble conditions. Configure this parameter to P to enable the entering of a passcode at the keypad after the Silence key or Enter key is pressed.

Notice!
UL 985 requirements for Household Fire Warning System Units
To comply with UL 985 requirements for Household Fire Warning System Units, configure the fire alarm silence to require a passcode.

RPS Menu Location
User Configuration > User (Keypad) Functions > Silence Function

10.3.33 Custom Function

Default: Passcode (P)
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.
– Passcode (P) - Require a passcode to enable this function panel wide.

This function allows the user to execute Custom Functions from the Shortcut Menu, A-Key, B-Key, or C-Key.
For the user to execute Custom Functions using a Keyfob, the user must have an associated Authority Level set to E.
The B6512 supports Custom Function 128 to 133.
The B5512 supports Custom Function 128 to 131.
The B4512 supports Custom Function 128 to 129.
The B3512 supports Custom Function 128.

RPS Menu Location
User Configuration > User Keypad Functions > Custom function

10.3.34 Keypad Programming

Default: P
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.
– Passcode (P) - Require a passcode to enable this function panel wide.

Note that Enable (E) is not available as a selection for the Keypad Programming parameter.
This function allows programming from keypads for a select list of parameters.
Only the installer passcode has authority for keypad programming.
If any one area is armed or the control panel is connected to RPS, you cannot access keypad programming.

RPS Menu Location
User Configuration > User Keypad Functions > Keypad Programming

Further information
Refer to the control panel documentation for more information on keypad programming.

10.4 Authority Levels

Authority Levels determine the features and functions to which users have access. The parameters in this section are used for configuring Authority Levels 1-14. Authority Level 15 is reserved for the Installer Passcode (User 0) and cannot be changed.
Use the User Configuration > User Assignments (passcodes) > *Area Authorities, page 152* parameter to assign users to an Authority Level for each area.

10.4.1 Authority Level Name (first language)

Default: Auth Level 1 (to 15)
Selections: up to 32 characters.
Enter up to 32 characters to describe the area.
The first language and the second language are programmed during panel account setup. Supported languages include English, Spanish, French, Brazilian Portuguese, Chinese, Polish, Italian, Greek, Hungarian, German, Dutch, and Swedish.

RPS Menu Location
User Configuration > Authority Levels > Authority Level Name

10.4.2 Authority Level Name (Second Language)

Default: Auth Level 1 (to 15)
Selections: up to 32 characters.
Enter up to 32 characters to describe the area.
The first language and the second language are programmed during panel account setup. Supported languages include English, Spanish, French, Brazilian Portuguese, Chinese, Polish, Italian, Greek, Hungarian, German, Dutch, and Swedish.

RPS Menu Location
User Configuration > Authority Levels > Authority Level Name (second language)

10.4.3 One-Time Disarm

Default: -
Selections:
– Enabled (E)
– Disabled (-)

Set this parameter to designate temporary access for a user to any areas assigned to this Authority Level. The temporary authority level does not expire on any date or time period. Users assigned an Authority Level with One-Time Disarm enabled, can only use their passcode once in each assigned area. When the same area is re-armed, One-Time Disarm expires and the User Authority Level for the area is set to 0: Unassigned.
Individual user permissions continue to use the permission set for the Authority Level.

RPS Menu Location
User Configuration > Authority Levels > One-Time Disarm

10.4.4 Disarm Select

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

These disarming functions are available to the user with this authority:
– Disarm All - disarms all areas within the scope of the keypad and included in the user's authority.
– Disarm Area# - Disarms only the selected area.

RPS Menu Location
User Configuration > Authority Levels > Disarm Select

10.4.5 All On Delay

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to arm the areas within the scope of the keypad and included in the user's authority level All On Delay (arm Part On points and Interior points with exit delay time and entry delay time).
If a user uses Command 1 to arm All On Delay, only the area the keypad is assigned to arms.
If a user arms All On Delay using the Remote Security Control app (RSC), all areas in the user’s Authority Level are armed.

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

10.4.6 All On Instant

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to arm the areas within the scope of the keypad and included in the user's authority level All On Instant (arm Part On and Interior points with no exit delay time and no entry delay time).
If a user uses Command 1 1 to arm All On Instant, only the area the keypad is assigned to arms.
If a user arms All On Instant, using the Remote Security Control app (RSC), all areas in the user’s authority level are armed.

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

10.4.7 Part On Instant

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to arm the areas within the scope of the keypad and included in the user's authority level Part On Instant (arm Part On points with no exit delay time and no entry delay time).

If a user uses Command 2 to arm Part On Instant, only the area the keypad is assigned to arms.

If a user arms Part On Instant using the Remote Security Control app (RSC), all areas in the user’s authority level are armed.

RPS Menu Location

User Configuration > Authority Levels > Part On Instant

10.4.8 Part On Delay

Default:

– Enabled (E) - Authority Levels 1-4
– Blank (-) - Authority Levels 5-15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to arm the areas within the scope of the keypad and included in the user's authority level Part On Delay (arm Part On points with exit delay time and entry delay time).

If a user uses Command 3 to arm Part On Delay, only the area the keypad is assigned to arms.

If a user arms Part On Delay using the Remote Security Control app (RSC), all areas in the user’s Authority Level are armed.

RPS Menu Location

User Configuration > Authority Levels > Part On Delay

10.4.9 Watch Mode

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to toggle watch mode on and off in the areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Watch Mode

10.4.10 View Area Status

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users with arm/disarm authority to view the arm/disarm and ready to arm status for areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location
User Configuration > Authority Levels > View Area Status

10.4.11 View Event Memory

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to view event memory for areas within the scope of the keypad and included in the user's authority level.
The control panel clears event memory when areas are armed.

RPS Menu Location
User Configuration > Authority Levels > View Event Memory

10.4.12 View Point Status

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to view the point status (normal, short, open) for areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location
User Configuration > Authority Levels > View Point Status

10.4.13 Walk Test (All Non-Fire Burg Points)

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to walk test controlled points (test without sending alarm reports to the central station receiver).
At the start of the walk test, the alarm bell output activates for 2 seconds. As the user faults each controlled point, the keypads beep once.
Fire points, gas points, and 24 hour points cannot be tested using this walk test user function.

RPS Menu Location
User Configuration > Authority Levels > Walk Test (non-fire burg points)

10.4.14 Walk Test All Fire Points

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to initiate a Fire walk test for fire points and gas points.

Notice!

Fire walk test includes gas and environmental points

When you perform a Fire Walk Test, the security system tests any 24-hour points that are not invisible. The Fire Walk Test includes gas, environmental (water, high temp, low temp) and any uncontrolled visible points.

When a Fire Walk Test starts

– The control panels sends a FIRE WALK START report to the central station receiver.
– There is local alarm annunciation only, no alarm reports are sent to the central station receiver.
– The control panel is powered by the battery only.
– The *Fire Bell, page 135* output activates for 2 seconds for each fire point or gas point that is tested.
– All fire points and gas points with the *Resettable, page 214* parameter set to YES, automatically reset when tested. [SENSORS RESETTING] shows at keypads.
– The keypad shows the point text for each point as each it is tested, and an updated "points tested" count.
– The test ends after all points are tested or after 20 minutes of no activity. The control panel sends a FIRE WALK END report to the central station receiver.

If fire points or gas points are faulted when Fire Walk Test ends, the points are bypassed and the trouble tone sounds. The keypads show the bypassed points and the trouble condition.

When a Fire Drill starts

– The control panel sends a FIRE DRILL START report to the central station receiver.
– The *Fire Bell, page 135* output activates until a user ends the drill by silencing the Fire Bell.
– Fire points and gas points are active. An alarm on a fire point or gas point ends the drill. The control panel sends Fire alarm reports.

When the fire drill ends, the control panel sends a FIRE DRILL END report.

RPS Menu Location

User Configuration > Authority Levels > Walk Test All Fire Points

10.4.15 Walk Test All Invisible Burg Points

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to test invisible points (the Invisible Point parameter set to Yes) without sending alarm reports to the central station receiver.
24-Hour points left faulted when exiting the Invisible Walk Test are bypassed. The trouble tone sounds at keypads.
Fire points and gas points cannot be tested using this Walk Test Invisible user function.

RPS Menu Location
User Configuration > Authority Levels > Walk Test All Invisible Burg Point

10.4.16 Service Walk All Points

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to use the Service Walk Test. The Service Walk Test includes all points that are assigned to a Source (the Source parameter is not set to Unassigned).
As the user faults each point, the keypads beep once.
Fire points, gas points, or 24-Hour points left faulted when exiting the Service Walk Test are bypassed. The trouble tone sounds at keypads.

RPS Menu Location
User Configuration > Authority Levels > Service Walk All Points

10.4.17 Send Report (Test / Status)

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to send a test report from keypads assigned to an area included in the user's authority level.

RPS Menu Location
User Configuration > Authority Levels > Send Report (Test/Report)

10.4.18 Cycle Door

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to cycle a door in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location
User Configuration > Authority Levels > Cycle Door

10.4.19 (Un)Lock door

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to use the lock and unlock door functions for doors in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > (Un)Lock Door

10.4.20 Secure Door

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to use the secure door function for doors in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Secure Door

10.4.21 Change Keypad Display

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to change keypad displays (bright display, dim display) for keypads in areas included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Change Keypad Display

10.4.22 Change Date and Time

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to change the control panel the date and time.

RPS Menu Location

User Configuration > Authority Levels > Change Date and Time

10.4.23 Change Passcode

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to change their own passcode.
To allow users to change passcodes for other users, refer to *Add User Passcode / Card / Level, page 173*.

RPS Menu Location

User Configuration > Authority Levels > Change Passcode

10.4.24 Add User Passcode / Card / Level

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to add and change (edit) other users. They can edit user passcode, name, authority level, keypad, access card (or token), language, and access to a Bosch mobile app.

RPS Menu Location

User Configuration > Authority Levels > Add User Passcode/Card/Level

10.4.25 Delete User Passcode / Card/ Level

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to delete other users.

RPS Menu Location

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

10.4.26 Extend Close

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to change the closing time in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Extend Close

10.4.27 View Event Log

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to view all events in the control panel event log.

RPS Menu Location

User Configuration > Authority Levels > View Event Log

10.4.28 User Command 7

Default:

– Enabled (E) - Authority Levels 1
– Blank (-) - Authority Level All others

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter enables user Command 7 for users.

RPS Menu Location

User Configuration > Authority Levels > User Command 7

10.4.29 User Command 9

Default:

– Enabled (E) - Authority Levels 1
– Blank (-) - Authority Level All others

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter enables user Command 9 for users.

RPS Menu Location

User Configuration > Authority Levels > User Command 9

10.4.30 Bypass a Point

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to bypass points in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Bypass a Point

10.4.31 Unbypass a Point

Default:

– Enabled (E) - Authority Levels 1-4, 15

– Blank (-) - Authority Levels 5-14

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to unbypass points in areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Unbypass a Point

10.4.32 Reset Sensor(s)

Default:

– Enabled (E) - Authority Levels 1-4, 15

– Blank (-) - Authority Levels 5-14

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to reset sensors.

RPS Menu Location

User Configuration > Authority Levels > Reset Sensors

10.4.33 Change Output(s)

Default:

– Enabled (E) - Authority Levels 1, 2, 15

– Blank (-) - Authority Levels 3-14

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to manually set and reset outputs.

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 in Enter Key Output.

Manual control (on/off) of outputs

Outputs based on Output Profiles can be turned on manually (by keypad or remotely) and will remain on.

Manually turn off outputs to return to automatic operation.

RPS Menu Location

User Configuration > Authority Levels > Change Outputs

10.4.34 Remote Program

Default:

– Enabled (E) - Authority Levels 1-4, 15

– Blank (-) - Authority Levels 5-14

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to start remote programming sessions. If users start this function when the phone line shared with the control panel is ringing, the control panel seizes the phone line.

RPS Menu Location
User Configuration > Authority Levels > Remote Programming

10.4.35 Go to Area

Default:
Enabled (E) - Authority Levels 1, 2, 15
Blank (-) - Authority Levels 3-14
Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.
This function temporarily assigns keypads to a different area.
Users are limited to functions enabled by their authority level for the area that the keypad is temporarily assigned to.
After 15 seconds of no user activity at the keypad, the keypad reverts back to it's assigned area.

RPS Menu Location
User Configuration > Authority Levels > Go to Area

10.4.36 Display Panel Type and Revision

Default:
– Enabled (E) - Authority Levels 1, 15
– Blank (-) - Authority Levels 2-14
Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.
This parameter allows users to display the control panel firmware revision. Keypads show the firmware revision in this format ##.##.###.

RPS Menu Location
User Configuration > Authority Levels > Display Panel Type and Revision

10.4.37 Change Skeds

Default:
– Enabled (E) - Authority Levels 1, 15
– Blank (-) - Authority Levels 2-14
Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.
This parameter allows users to change (edit) skeds.
Skeds can be restricted from being edited by setting the Schedules > Skeds > *Time Edit, page 233* parameter to No.

RPS Menu Location
User Configuration > Authority Levels > Change Skeds

10.4.38 Custom Function

Default:
– Enabled (E) - Authority Level 1
– Blank (-) - Authority Levels 2-15
Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to use Custom Functions.

Notice!

User authority for custom functions overrides authority for the user functions within

When a user does not have authority for a function through the keypad menu, it does not prevent the function from running within a custom function.

RPS Menu Location

User Configuration > Authority Levels > Custom Function 128 to #

10.4.39 Force Arm

Default:

– Enabled (E) - Authority Levels 1-6
– Blank (-) - Authority Levels 7-15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to force arm the control panel.

RPS Menu Location

User Configuration > Authority Levels > Force Arm

10.4.40 Send Area Opening/Closings

Default:

– Enabled (E) - Authority Level 1-14
– Blank (-) - Authority Level 15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter enables opening and closing reports for users in areas included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Send Area Opening/Closings

10.4.41 Restricted Open/Close

Default: Blank (-) for all authority levels

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter restricts opening and closing reports for users in areas included in the user's authority level. The control panel sends opening reports only when the alarm bell is active when the user disarms. The control sends closing reports only when the user force arms or bypass arms.

Areas to which this authority level is assigned must be programmed for restricted openings and closings (Refer to Area Wide Parameters > *Restricted O/C, page 108*).

RPS Menu Location

User Configuration > Authority Levels > Restricted Open/Close

10.4.42 Part On Open/Close

Default:

– Enabled (E) - Authority Levels 1 - 14
– Blank (-) - Authority Level 15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter enables opening and closing reports when users arm Part On and disarm for users in areas included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Part On Open/Close

10.4.43 Send Duress

Default:

– Enabled (E) - Authority Level 14
– Blank (-) - Authority Levels 1-13, 15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter enables duress reports for users when the Area Parameters > Duress Enable parameter is set to Yes for areas included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Send Duress

10.4.44 Arm by Passcode

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to enter their passcode to arm areas within the scope of the keypad and included in the user's authority level.

RPS Menu Location

User Configuration > Authority Levels > Arm by Passcode

10.4.45 Disarm by Passcode

Default:

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

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.
– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to enter their passcode to disarm areas within the scope of the keypad and included in the user's authority level.

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:

– User Configuration > Authority Levels > Disarm
– User Configuration > Authority Levels > Send Duress
– And this parameter Disarm by Passcode

Configure the Area Wide Parameters > Duress Enable parameter to Yes in applicable areas, or the keypad will respond with No Authority.

Further information

– *Disarm Select, page 166*
– *Send Duress, page 178*

RPS Menu Location

User Configuration > Authority Levels > Disarm by Passcode

10.4.46 Security Level

Default:

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

Selections:

– All On (A) - Users have access rights for this area when the area in any armed state.
– Part On (P) - Users have access rights for this area when the area is Part On or disarmed, but not when the area is all on Armed.
– Disarmed (D) - Users have access rights for this area only when it is disarmed.
– No Access (-) - Users do not have access rights to this area.

RPS Menu Location

User Configuration > Authority Levels > Security Level

10.4.47 Disarm Level

Default:

Disarm (D) - Authority Levels 1-5

No Disarm Rights (-) - Authority Levels 6-15

Selections:

– All On or Part On to Part On, Instant (I) - when users present their access credential (card or token) and the area is All On, Delay (or Instant) or Part On, Delay, the area goes to Part On, Instant. The Authority Level > Security Level parameter must be set to All On (A) for the area.
– Disarm (D) - when users present their access credential (card, token or passcode when Keypad Passcode Enter Function is set to Cycle Door) and the area is All On, Delay (or Instant) or Part On, Delay (or Instant), areas within the scope of the keypad and included in the user's authority level change to disarmed.

– No Disarm (-) - users cannot present their access credential (card or token) to disarm.

For more information on programming this prompt for a Shared area, see the Access Control Readers Assigned to the Shared Area paragraph for the *Area Type, page 100* prompt in Area Parameters.

Notice!
Burglar bells silenced when user presents token/card
Burglar bells are silenced when a user presents a token, card or passcode when configured to Cycle Door.
Burglar bells are silenced in the local area when a user disarms with a token, card or passcode when configured to Cycle Door or presents a token, card or passcode when configured to Cycle Door during an alarm. The user must use a passcode to silence a fire bell. Cancel reports are sent after a valid passcode or token/card has silenced the bell.

Notice!
Authority Level 15 reserved
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 > Disarm Level

10.4.48 Function Level

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

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

Users must have a passcode assigned to start a custom function with an access card or token.
Users do not require Security Level or Disarm Level authority to start a custom function with an access card or token.
When users who have both Disarm Level authority and Function Level authority present a card or token, the Disarm Level is applied first and then the Function Level (the area disarms and then custom function starts).

RPS Menu Location
User Configuration > Authority Levels > Function Level

10.4.49 Keyfob Arm

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

Selections:
– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to arm areas included in the user's authority level using a RADION wireless keyfob.

Duress operation when arming is not applicable when using RADION wireless keyfobs.

RPS Menu Location

User Configuration > Authority Levels > Keyfob Arm

10.4.50 Keyfob Disarm

Default:

– Enabled (E) - Authority Levels 1-6

– Blank (-) - Authority Levels 7-15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows users to disarm areas included in the user's authority level using a RADION wireless keyfob.

Duress operation when disarming is not applicable when using RADION wireless keyfobs.

RPS Menu Location

User Configuration > Authority Levels > Keyfob Disarm

10.4.51 Firmware Update

Default:

– Enabled (E) - Authority Levels 1 - 6

– Blank (-) - Authority Levels 7 - 15

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

When local authorization is required, only a security user with the Firmware Update authority level can authorize the update.

RPS Menu Location

User Configuration > Authority Levels > Firmware Update

10.4.52 Silence Function

Default:

– Enabled (E) - Authority Levels 1 and 15

– Blank (-) - Authority Levels 2-14

Selections:

– Blank (-) - this function is not enabled for users that are assigned to this authority level.

– Enabled (E) - this function is enabled for users that are assigned to this authority level.

This parameter allows the silencing of trouble tones at keypads for areas within the scope of the keypad and included in the user’s authority level.

10.5 Passcode Security

Configurable options that secure system access after failed passcode attempts through automation or keypads.

10.5.1 Network

Enable

Default: Yes

Selections:

– Yes - passcode automatic lock out enabled.

– No - passcode automatic lock out disabled.

Use this parameter to enable passcode security for panel automation. Network passcode automatic lockout applies to remote Network, Cellular, IP Direct, Webconnect_Cell, Cloud, Cellular Callback and local USB connections.

An error message shows to the operator when the maximum number of invalid passcode attempts are reached. The message shows until the lockout duration completes. After the lockout duration completes, RPS can then connect to a panel using valid credentials.

Failed Attempt

Default: 15

Selections: 0-21

Use this parameter to set the number of failed passcode attempts that can occur before automation connections are locked for a set duration.

The Failed Attempt count will increment each time an invalid passcode is entered that is different than the prior invalid attempt.

If Failed Attempt is set to 0, the Network passcode automatic lockout is disabled.

Lockout Duration

Default: 900 (seconds)

Selections: 0-65535 (seconds)

Use this parameter to set the amount of time in seconds that the automation software will be locked when the set number of passcode failed attempts is reached.

RPS Menu Location

User Configuration > Passcode Security > Network

10.5.2 Keypad

Enable

Default: Yes

Selections:

– Yes - passcode automatic lock out enabled.

– No - passcode automatic lock out disabled.

Use this parameter to enable Passcode Security for Keypad operations.

Failed Attempt

Default: 6

Selections: 0-21

Use this parameter to set the number of failed password attempts that can occur before the keypad is locked for a set duration.

The Failed Attempt count increments each time an invalid passcode is entered that is different from the prior invalid attempt.

Lockout Duration

Default: 0 (not locked out)

Selections: 0-65535

Use this parameter to set the amount of time in seconds that a keypad is locked out when the set number of passcode failed attempts is reached.

RPS Menu Location

User Configuration > Passcode Security > Keypad

11 Points

For Points online videos see:
– Navigation improvements
Available Online Resources: Instructional & Overview Videos

11.1 Point Assignments

11.1.1 Source

Default:
– On-board - Points 1-8
– Unassigned - all other points

Selections:
– Unassigned - point is not in use.
– Octo-input - point is installed on B208 Octo-input module.
– Wireless - point is installed on an SDI2 bus RF receiver.
– On-board - point is installed on the control panel (points 1-8).
– Output - point is connected in logic to the output of the same number. No physical device associated with this point.
– Keypad - point is installed on an SDI2 bus keypad.
– IP Camera - point represents input from an IP Camera Video Content Analytics. Control panels support assigning up to 10 points per IP camera, including up to 2 wired inputs and 8 virtual task alarms. The panel points available are specific for each IP camera.
– Door - point is installed on a door controller module.

Use this parameter to assign points to physical devices. When a selection is grayed out, you cannot assign the point to that device.
Point Source for points 1-8 is fixed as On-board and cannot be changed.
For IP cameras, use *Camera Inputs-Outputs, page 44* to assist in assignment of panel points and panel outputs.

RPS Menu Location
Points > Point Assignments > Source

11.1.2 Text (first language)

Default: Point #

Selections:
– Up to 32 characters - spaces before, after and within a string of text are treated as text and are included in the 32 character limit.

Enter up to 32 characters of text, numbers, and symbols to describe the point. The point text shows at keypads and is included in point reports sent to the central station receiver (Modem4 reporting format only).
Keypads show the first 20 characters. If the text is more than 20 characters, the complete text scrolls across the display one time. To scroll the text again, press [ESC].

Including the point number can help
Including the point number in the point text helps users when they are viewing events, initiating functions and commands, and troubleshooting.

RPS Menu Location
Points > Point Assignments > Text

11.1.3 Text (second language)

Default: blank

Selections:

– Up to 32 characters - spaces before, after and within a string of text are treated as text and are included in the 32 character limit.

Enter up to 32 characters of text, numbers, and symbols to describe the point. The point text shows at keypads and is included in point reports sent to the central station receiver (Modem4 reporting format only).

Keypads show the first 20 characters. If the text is more than 20 characters, the complete text scrolls across the display one time. To scroll the text again, press [ESC].

Including the point number can help

Including the point number in the point text helps users when they are viewing events, initiating functions and commands, and troubleshooting.

RPS Menu Location

Points > Point Assignments > 2nd Language Text

11.1.4 Profile (Index)

Default:

– Smoke Detector (4) - point 1
– Part On: Delay (8) - point 2, point 3
– Interior: Follower (13) - point 4, point 5
– Part On: Instant (7) - point 6, point 7
– 24-hr Instant on Open/Sort (1) - point 8
– Disabled (0) - all other points

Selections:

– 0-20

Use this parameter to select a Point Profile for each point. The Point Profile determines how the control panel responds to changes of point status (faulted, normal, trouble, missing, armed, disarmed).

When the point Source parameter is set to disabled and the point is assigned a Profile, the control panel creates a MISSING POINT event.

When the point Source parameter is not set to 0 and the Point Profile is set to disabled, the control panel creates an EXTRA POINT event.

If a Point Profile is assigned to a point device that has an incorrect address or that is not connected to the SDI/SDI2 bus, or if a Wireless point device fails to check-in, a MISSING POINT response occurs.

When a point goes missing, the control panel generates the following responses based on the point type:

– Fire and Gas points generate missing trouble responses.
– Non-fire/Gas 24-hour points generate missing alarm responses.
– Non-fire/Gas, non 24-hour points generate missing alarm responses while armed, and missing trouble responses while disarmed. The exception is when Non-fire/gas, non-24-hour points with a point response of 9 to D generate a missing alarm response while disarmed.
– Supervisory points generate missing supervisory responses.

If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location
Points > Point Assignments > Index

11.1.5 Area

Default: 1: Area 1
Selections:
– 1-6 - B6512
To assign a point to an area, select the area number.
If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location
Points > Point Assignments > Area

11.1.6 Debounce

Default: 500 ms
Selections:
– 250 ms
– 500 ms
– 750 ms
– 1.00 s
– 1.25 s
– 1.50 s
– 1.75 s
– 2.00 s
... to ...
– 6.00 s
The Debounce parameter sets the length of time the control panel scans a point before making a fault.
For B Series, Bosch recommends an entry of 500 ms or higher. For Interior Follower points set Debounce to at least 750 ms seconds.
When the point *Source, page 183* is set to Wireless, IP Camera, or Output, the programmer automatically sets the Debounce parameter to dash (-) to show the parameter does not apply.
Consult the manufacturer's instructions for the device connected to the point if you are unsure of how to set this parameter.

RPS Menu Location
Points > Point Assignments > Debounce

11.1.7 Output

Default: 0: Unassigned
Selections:
– 0 (disabled), 1 to 96
Use this parameter to activate an output when the point goes into alarm. The output does not activate for Trouble or Supervisory events.
The output resets when the alarm associated with a point output is cleared from the keypad.
If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

Notice!

Legacy BFSK Relay or Relay functionality

The point assignment parameters for many legacy Bosch control panels include a BFSK Relay or Relay parameter for each point.

You can emulate BFSK Relay functionality by setting this Output parameter to the same output number for multiple points.

RPS Menu Location

Points > Point Assignments > Output

11.1.8 RADION RFID (B810)

Default: - blank

Selections: 0, 11 - 167772156

The RFID (Radio Frequency Identification) number is a unique number assigned to wireless devices at the factory.

When the point Source parameter is set to Wireless, the programmer sets this RFID parameter to 0. The RFID can be Auto-Learned through an SDI2 bus RF receiver, or it can be entered here.

The RFID can be edited for point replacement, or can be set to 0 to disable an RF point.

Programmer enforced wireless limits

Setting the *Wireless Module Type, page 266* parameter to B810 RADION Wireless limits the control panel to 1512 wireless devices: 1000 keyfobs, 504 points (point Source parameter set to Wireless), and 8 repeaters.

RPS Menu Location

Points > Point Assignments > RADION RFID (B810)

11.1.9 RADION Device Type

Default: Blank

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
- Panic, Fixed Position
- Heat

Each RADION device type includes four input functions. Refer to the following table.

Device type	Input Function 1	Input Function 2	Input Function 3	Input Function 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
Panic, Fixed Position	Not used	Not used	Not used	Not used
Heat	Heat alarm	Not used	Not used	Not used

When you select the device type, you can enable or disable input functions by clicking the corresponding checkbox in the dialog box.
The programmer resets input functions to their default value when the wireless device type changes.

RPS Menu Location
Points > Point Assignments > RADION Device Type

11.1.10 Inovonics RFID (B820)

Default: N/A
Selections: 0 - 167772156
The RFID (Radio Frequency Identification) number is a unique number assigned to wireless devices at the factory.
When the point Source parameter is set to Wireless, the programmer sets this RFID parameter to 0. The RFID can be Auto-Learned through an SDI2 bus RF receiver, or it can be entered here.
The RFID can be edited for point replacement, or can be set to 0 to disable an RF point.

Programmer enforced wireless limits
Setting the *Wireless Module Type, page 266* parameter to B820 Inovonics Wireless limits the control panel to 350 wireless devices, not including repeaters. The sum of the number points (point Source parameter set to Wireless) plus the number keyfobs cannot be greater than 350.

RPS Menu Location
Points > Point Assignments > RFID (B820 Inovonics Wireless)

11.2 Cross Point Parameters

11.2.1 Cross Point Timer

Default: 20
Selections: 5-255 (seconds)
This parameter sets the time the control panel waits after a fault on a Cross Point for a second point in the same Cross Point Group to fault before creating a Cross Point Alarm Event. If a second point is not faulted within the Cross Point Time, then an alarm event is not generated.

Notice!
Non-fire points only
Only use the Cross Point function on non-fire points.

Supported Point Type parameters
- 24 hour
- Interior
- Interior follower
- Part On
- High Temp
- Low Temp
- Water

RPS Menu Location
Points > Cross Point Parameters > Cross Point Timer

11.3 Point Profiles

Point profiles (point indexes) determine how the control panel responds to changes on points. To build point profiles, use the parameters in this section. Assign Point Profiles to points in Point Assignments.

Notice!
New point configurations not supported with older panel firmware versions
Sending point configurations to earlier panel firmware versions that do not support those configurations will not behave as intended. The panel will update unsupported point types to the default point type and alarm conditions will trigger a point trouble event.

11.3.1 Point Profile Text (first language)

Default:
- Point Profile 1 - 24-hr Inst Open/Short (24-hour, instant on open or short)
- Point Profile 2 - 24- hr Inv/Slt on Shrt (24-hour, invisible and silent on short)

- Point Profile 3 - Pull Station
- Point Profile 4 - Smoke Detector
- Point Profile 5 - Smoke w/Verification (Smoke detector with verification)
- Point Profile 6 - Bell Suprv - D192G (Bell supervision for D192G)
- Point Profile 7 - Part On: Instant
- Point Profile 8 - Part On: Delay
- Point Profile 9 - Prt:Inst,Lcl Darm,Buz (Part, instant, local while disarmed, buzz)
- Point Profile 10 - Interior: Instant
- Point Profile 11 - Interior: Delay
- Point Profile 12 - Intr:Inst, Lcl Disarm (Interior, instant, local while disarmed)
- Point Profile 13 - Interior: Follower
- Point Profile 14 - Maintained Keyswitch
- Point Profile 15 - Momentary Keyswitch
- Point Profile 16 - Point Opening/Closing on Fault
- Point Profile 17 - Gas
- Point Profile 18 - Gas Supervisory
- Point Profile 19 - Aux AC Supervision
- Point Profile 20 - Part On: Watch Off

Selections: Up to 24 alphanumeric characters

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

RPS Menu Location

Points > Point Profiles > Point Profile Text

11.3.2 Point Profile Text (Second Language)

Default: Blank

Selections: Up to 24 alphanumeric characters

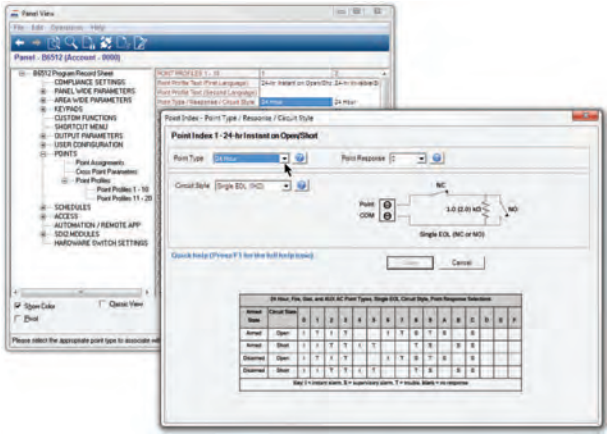
Enter up to 24 characters of text to describe the point profile (point index).

RPS Menu Location

Points > Point Profiles > Point Profile Text (second language)

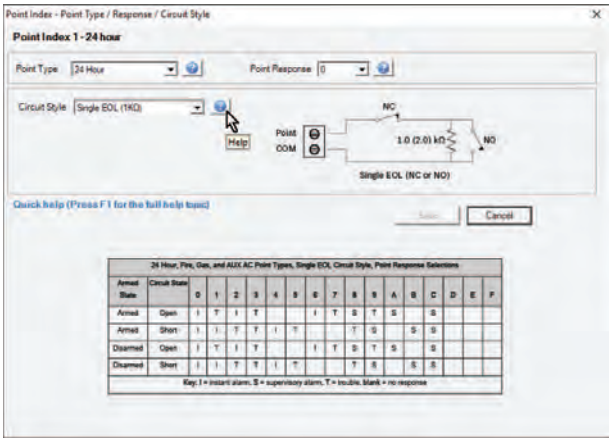
11.3.3 Point Type/Response/Circuit Style

Showing the Point Type, Point Response, and Circuit Style parameters in a single window allows you to see the interaction between the three parameters.



The Point Response parameter and the Point Type parameter together determine how the control panel responds to changes on point sensor loops (open, short, normal) for wired points, or changes in point states for wireless point devices (fault, normal, trouble).

To see help for the individual parameters, press the individual help buttons in the window.



11.3.4 Point Type

Default:

- 24 Hour - Point Profiles 1-2, 6
- Part On - Point Profiles 7-9, 20
- Interior - Point Profile 10-12
- Interior Follower - Point Profile 13
- Keyswitch Maintained - Point Profile 14
- Keyswitch Momentary - Point Profile 15
- Open/Close Point - Point Profile 16
- Fire Point - Point Profile 3-5
- AUX AC Supervision - Point Profile 19
- Gas Point - Point Profile 17, 18

These point types are also available for use, but do not have default Point Profiles assigned:

- Panic

Environmental point types:

- Water
- High Temp
- Low Temp

The Point Type parameter sets the point type for the point profile.

Selections:

- **24 Hour**

24-hour points are armed all the time. They can be used for panic, medical, and police alerts.

If you make a 24-hour point bypassable (set the *Bypassable, page 211* parameter to Yes), set the *Buzz on Fault, page 208* parameter to 1, 2, or 3, and set the *Report Bypass at Occurrence, page 212* parameter to Yes (if an area is never armed, deferred bypass reports would never be sent).

Notice!
UL requirement for hold-up devices
For hold-up devices in UL installations, use the 24-Hour point type. The Point Text must include, “hold-up”.

Notice!
Fire door, roof hatch, and similar applications
For fire doors, roof hatches, and similar applications needing 24 hour monitoring, consider using the Part On point type. 24-hour points do not show faulted or bypassed status when arming an area, Part On points do.
Set the *Point Response, page 195* parameter to 9, A, B, C, D, or E.
Consider enabling the Buzz On Fault parameter and the *Local While Disarmed, page 210* parameters.

– **Part On**

Part On points are typically assigned to devices in the perimeter of the premises (doors and windows).
When a user arms an area All On; Part On points, Interior points, and Interior Follower points are all armed.
When a user arms an area Part On; only Part On points are armed. Interior points, and Interior Follower points are not armed. In a typical system, turning an area Part On arms only the perimeter protection allowing users to remain in the premises without creating alarm events from interior points.
The Points > Point Profile > Point Response parameter determines if Part On points include entry delay time, or create an alarm event immediately when faulted.
Entry delay time allows users to reach a keypad and disarm without making an alarm event. For example, when a user opens the front door (faulting a Part On point) entry delay time begins. The user goes to a keypad and disarm (change the area to off) before exit delay time expires preventing an alarm event.
If the area is in entry delay and a second Part On point trips, the control panel compares the remaining entry delay time to the entry delay time programmed for the second Part On point. If the second point's entry delay time is less than the remaining time, it shortens the entry delay time.

Notice!
Part On Points with instant Point Response create immediate alarm events
Perimeter Points programmed for an instant *Point Response, page 195* do not start entry delay time when fauted. They generate an alarm event immediately, even during entry or exit delay.

– **Interior**

Interior points are typically used to monitor interior detection devices such as interior doors and motion detectors.
Interior points are armed only when the area is All On. They are not armed when the area is Part On.
The Points > Point Profile > Point Response parameter configures Interior points for instant or delayed alarm response. Interior points are typically configured for instant alarm response.

Notice!
Interior Points with instant Point Response create immediate alarm events
Interior Points programmed for an instant *Point Response, page 195* are faulted, they make alarm events immediately, even during entry or exit delay.

When an interior point configured for delayed alarm response is faulted while the area is All On, it starts entry delay time. It will not make an alarm event unless entry delay time ends before the area is disarmed.
If an interior point programmed for delayed point response is faulted when entry delay time is already started, the control panel compares the remaining entry delay time to the entry delay time programmed for the interior point. If the interior point's entry delay time is less than the remaining time, the control panel shortens the entry delay time.

Notice!
Use the *Interior Follower, page 219* point type for instant alarm if the area is not in entry delay
For some installations, you may want an interior point that follows, but does not start entry delay.

– **Interior Follower**

Interior Follower points are typically used to monitor interior detection devices such as interior doors and motion detectors.
Interior Follower points are armed only when the area is All On. They are not armed when the area is Part On.
Faulting an Interior Follower point while the area is All On creates an instant alarm event. If entry delay time is started by another point before the interior follower point is tripped, the interior follower point delays the alarm event until exit delay time expires. If the area is disarmed before entry delay time ends, there is no alarm event.
During Exit Delay, faulting an Interior Follower point does not create an alarm event.
Interior Follower points do not start entry delay even when configured for a delayed alarm response (*Point Response, page 195* parameter set to 4, 5, 6, 7, or 8).

Notice!
Use the Interior point type and delayed alarm response for interior points that initiate entry delay
For some installations, you may want an interior point that starts entry day. Faulting an Interior point configured for delayed alarm response (refer to *Point Response, page 195*) while the area is All On starts entry delay. The alarm response is delayed until exit delay time ends. If the area is disarmed before entry delay time expires, there is no alarm response.

– **Keyswitch Maintained**

Keyswitch Maintained points are used for arming (All On) and disarming areas.
For Keyswitch Maintained points, when the Points >Point Profiles > Point Response parameter is set to 1:

- When the point state is **normal** the area is disarmed (Off).
- When the point state changes from normal to **open**, the area arms to All On.
- When the point state changes from open to normal the area disarms (goes to Off).
- If the point state changes to **short** when the area is armed (All On or Part On) the control panel makes a point alarm event. If the points state changes to short when the area is disarmed (Off) the control panel makes a point trouble event. When the point state changes from shorted to normal or open, the trouble restores.

For Keyswitch Maintained points, when the Points >Point Profiles > Point Response parameter is set to 2:

- When the point state is **open** the area is disarmed (Off).
- When the point state changes from open to **normal**, the area arms to All On.

– When the point state changes from normal to open the area disarms (goes to Off).
– If the point state changes to **short** when the area is armed (All On or Part On) the control panel makes a point alarm event. If the points state changes to short when the area is disarmed (Off) the control panel makes a point trouble event. When the point state changes from shorted to normal or open, the trouble restores.

Trouble and restoral reports are not sent if the *Local While Disarmed, page 210* parameter is set to Yes.
Alarm and restoral reports are not sent if the *Local While Armed, page 210* parameters set to Yes.

Notice!
Point Response 2 is required for Inovonics FA113 Wireless devices.

– **Keyswitch Momentary**

Keyswitch momentary points are used for arming (All On) and disarming areas.
For keyswitch momentary points, set the Points > Point Profiles > Point Response parameter to 1.
Changing the point state of a keyswitch momentary point from **normal** to **short** to **normal** toggles the armed state of the area.
If the point state changes to **open** when the area is armed (All On or Part On) the control panel makes a point alarm event. If the points state changes to **open** when the area is disarmed (Off) the control panel makes a point trouble event. When the point state changes from open to normal, the trouble restores
Trouble and restoral reports are not sent if *Local While Disarmed, page 210* is set to Yes.
Trouble and restoral reports are not sent if *Local While Armed, page 210* is set to Yes.

– **Open/Close Point**

Open/close points arm and disarm independently of the area they are assigned to.
For open/close points, set the Points > Point Profiles > Point Response parameter to 1.
When the point state changes from **short** to **normal** the point arms. The control panels sends a POINT CLOSING report.
When the point state changes from **normal** to **short** the point disarms. The control panels sends a POINT OPENING report.
When the point state changes from **normal** to **open** the control panel creates a point alarm event.
When the point state changes from **short** to **open** the control panel creates a point trouble event.

POINT CLOSING reports are not sent if the *Local While Armed, page 210* parameter is set to Yes.
Point ALARM and RESTORAL reports are not sent if the *Local While Disarmed, page 210* parameter is set to Yes.
POINT OPENING reports are not sent if the *Local While Armed, page 210* parameter is set to Yes.
Local bells are silenced through the keypad.

– **Fire Point**

Use Fire points to monitor fire detection devices.
Fire alarms are the highest priority events in the control panel.

– **Aux AC Supervision**

Use Aux AC supervision points to monitor the AC power source of auxiliary power supply modules.
When the point state is off-normal, the control panel waits for the time programmed in the AC Fail Time parameter before making a point trouble event.
Aux AC supervision points do not use the *Point Response, page 195* parameter. There are no alarm events for Aux AC supervision points.
If Aux AC supervision points are bypassed, 24 HOUR PT BYPASSED shows on the keypads.

– **Gas Point**

Use Gas points to monitor gas detection devices.

– **Custom Function**

Use custom function points to activate custom functions.
Use the parameters in the *Custom Functions, page 128* section to configure custom functions.

– **Water Point**

Use Water point to monitor water detection devices.

– **High Temp**

Use High Temp to monitor high temperature detection devices.

– **Low Temp**

Use Low Temp to monitor low temperature detection devices.

– **Panic**

Use Panic to monitor for panic alarms. A Panic point operates the same as a 24 Hour point.

RPS Menu Location

Points > Point Profiles > Point Type / Response / Circuit Style

11.3.5 Point Response 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.

11.3.6 Point Response

Default:

	Point Profile									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Point Response Default	0	1	1	1	1	9	0	8	9	0

Table 11.1: B Series

	Point Profile									
	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Point Response Default	8	9	8	1	1	1	1	9	0	0

Selections: 0 - 9, A - F

Showing the Point Type, Point Response, and Circuit Style parameters in a single window allows you to see the interaction between the three parameters.
The Point Response parameter and the Point Type parameter together determine how the control panel responds to changes on point sensor loops (open, short, normal) for wired points, or changes in point states for wireless point devices (fault, normal, trouble).
The tables below show the Point Response selections for:

- 24 Hour, Fire, Gas, Panic, and AUX AC Supervision
- Controlled point types - Part On, Interior, and Interior Follower
- Keyswitch Maintained
- Keyswitch Momentary
- Open/Close Point
- Custom Function
- Water, High Temp, and Low Temp

Notice!
Changing Point Type automatically changes Point Response to default
Selecting a Point Type automatically changes the Point Response to the default for that Point Type.

24 Hour, Fire, Gas, Panic, and AUX AC Point Types Single EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	I	T	I	T			I	T	S	T	S		S			
Armed	Short	I	I	T	T	I	T			T	S		S	S			
Disarmed	Open	I	T	I	T			I	T	S	T	S		S			
Disarmed	Short	I	I	T	T	I	T			T	S		S	S			
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Example: Point Type = 24-hour and Point Response = 8. 24-hour point with supervisory response when open and a trouble response when shorted.

24 Hour, Fire, Panic, and Gas Point Types Dual EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	T	I	T	I												
Armed	Fault	I	I	S	S												
Disarmed	Open/ Short	T	I	T	I												
Disarmed	Fault	I	I	S	S												
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Example: Point Type = 24-hour and Point Response = 2. 24-hour point with supervisory response for fault and a trouble response for open or short.

24 Hour, Fire, Panic, and Gas Point Types, Single EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	TA	TA	TA	I	T			I	T							
Armed	Short	I	T	TA	TA	TA	I	T									
Disarmed	Open	TA	TA	TA	I	T			I	T							
Disarmed	Short	I	T	TA	TA	TA	I	T									
Key: I = instant alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Example: Point Type = 24-hour and Point Response = 4. 24-hour point with trouble response when open and a tamper alarm response when shorted.

24 Hour, Fire, Panic, and Gas Point Types, Dual EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	TA	TA	TA	TA												
Armed	Fault	I	T	TA													
Disarmed	Open/ Short	TA	TA	TA	TA												
Disarmed	Fault	I	T	TA													
Key: I = instant alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Example: Point Type = 24-hour and Point Response = 1. 24-hour point with trouble response for fault and a tamper alarm response for open or short.

Notice!
Control panel firmware requirements for Single EOL with Tamper and Dual EOL with Tamper circuit styles.
To use a Single EOL with Tamper or Dual EOL with Tamper circuit style, make sure the control panel firmware is v3.06 or greater.

Notice!
For Dual EOL Circuit Styles, purchase second 1kΩ **EOL separately**
Order ICP-1K22AWG-10, package of 10 resistors.

Notice!
For Dual EOL Circuit Styles, circuit states are normal, fault, short, open
Normal - the NC (normally closed) switch shown in the circuit diagram is closed.
Fault - the NC switch shown in the circuit diagram is open.
Short - the sensor loop is shorted.
Open - the sensor loop circuit is open.

Notice!
Control panel and B208 Octo-input firmware requirements for Dual EOL
To use the Dual EOL Circuit style, make sure the control panel firmware is v3.01 or greater. If you are using a B208 Octo-input Module, make sure the module firmware is v2.1.1 or greater.

24 Hour, Fire, Panic, and Gas Point Types, No EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Fault	I	T	S													
Disarmed	Fault	I	T	S													
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Example: Point Type = 24-hour and Point Response = 2. 24-hour point with supervisory response for fault and a trouble response for open or short.

Notice!
For the No EOL Circuit Style, circuit states are normal and fault,
in the Point Diagnostic window, circuit status is open or short
In the point response tables, the circuit states are normal and fault for the No EOL Circuit Style. The *Normal State, page 218* parameter defines the normal and fault circuit states. For No EOL circuit style points, the point diagnostics window shows open or short in the circuit status column.

Controlled Point Types, Single EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**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, **blank** = no response																	

Example: Point Type = Part On and Point Response = 8. Perimeter point with delayed alarm response when armed (opened or shorted) and no response when disarmed.

Controlled Point Types, Dual EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	I	I	I	I	I	I	I	I								
Armed	Fault	I	D	I	D	I	D	I	D								
Disarmed	Open/ Short	T	T	I	I	T	T	I	I								
Disarmed	Fault					T	T	T	T								
Key: I = instant alarm, **D** = delayed alarm, **T** = trouble, **blank** = no response																	

Example: Point Type = Part On and Point Response = 1. When the area is armed (All On, Part On), a fault on the point circuit creates a delayed alarm response. An open or short on the point circuit creates an instant alarm.
When the area is disarmed (Off), an open or short on the point circuit creates a point trouble. There is no response for a fault on the point circuit.

Controlled Point Types, Single EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	TA	TA	TA	TA	TA	TA	I	D	T	T	I	D				
Armed	Short	I	D	T	T	I	D	TA	TA	TA	TA	TA	TA				
Disarmed	Open	TA	TA	TA	TA	TA	TA				T	I	D				
Disarmed	Short				T	I	D	TA	TA	TA	TA	TA	TA				

Controlled Point Types, Single EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Key: I = instant alarm, **D** = delayed alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Example: Point Type = Part On and Point Response = 3. Perimeter point with tamper alarm response when open (armed or disarmed). Trouble response when short (armed or disarmed)

Controlled Point Types, Dual EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	TA	TA	TA	TA	TA	TA										
Armed	Fault	I	D	I	D	T	T										
Disarmed	Open/ Short	TA	TA	TA	TA	TA	TA										
Disarmed	Fault			T	T		I										
Key: I = instant alarm, **D** = delayed alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Example: Point Type = Part On and Point Response = 1. Perimeter point with tamper alarm response when shorted or opened (armed or disarmed). Delayed alarm response for fault (armed or disarmed).

Notice!
Control panel firmware requirements for Single EOL with Tamper and Dual EOL with Tamper circuit styles.
To use a Single EOL with Tamper or Dual EOL with Tamper circuit style, make sure the control panel firmware is v3.06 or greater.

Notice!
For Dual EOL Circuit Style, purchase second 1kΩ **EOL separately**
Order ICP-1K22AWG-10, package of 10 resistors.

Notice!
For Dual EOL Circuit Styles, circuit states are normal, fault, short, open
Normal - the N/C (normally closed) switch shown in the circuit diagram is closed.
Fault - the N/C switch shown in the circuit diagram is open.
Short - the sensor loop is shorted.
Open - the sensor loop circuit is open.

Notice!
Control panel and B208 Octo-input firmware requirements for Dual EOL
To use the Dual EOL Circuit style, verify the control panel firmware is v3.01 or greater.
If you are using a B208 Octo-input Module, verify the module firmware is v2.1.1 or greater.

Controlled Point Types, No EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Fault	I	I	D	D	T											
Disarmed	Fault		T		T	T											
Key: I = instant alarm, **D** = delayed alarm, **T** = trouble, **blank** = no response																	

Example: Point Type = Part On and Point Response = 2. When the area is armed (All On, Part On), a fault on the point circuit creates a delayed alarm response.
When the area is disarmed (Off), there is no response for a fault on the point circuit.

Notice!
For the No EOL Circuit Style, circuit states are normal and fault,
in the Point Diagnostic window, circuit status is open or short
In the point response tables, the circuit states are normal and fault for the No EOL Circuit Style. The *Normal State, page 218* parameter defines the normal and fault circuit states.
For No EOL circuit style points, the point diagnostics window shows open or short in the circuit status column.

Keyswitch Maintained Point Type, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open			D													
Armed	Short		I	I													
Disarmed	Open		A														
Disarmed	Short		T	T													
Key: A = transition from normal to open changes arming state to armed, **D** = transition from normal to open changes arming state to disarmed, **I** = instant alarm, **T** = trouble, **blank** = no response																	

When the point response is set to 1 and the point circuit is normal, the area is disarmed (Off). Changing the point circuit state from normal to open arms the area (All On). Changing the point circuit state from open to normal disarms the area (Off).
When the point response is set to 2 and the point circuit is normal, the area is armed (All On). Changing the point circuit state from normal to open disarms the area (Off). Changing the point circuit state from open to normal arms the area (All On).
A short on the point circuit creates a point trouble while the area is disarmed (Off). A short on the point circuit while the area is armed creates an instant alarm. When the point circuit returns to normal or open the trouble restores.

Keyswitch Momentary Point Type, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open		I														
Armed	Short		D														
Disarmed	Open		T														
Disarmed	Short		A														

Keyswitch Momentary Point Type, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Key: A = transition from normal to short to normal changes arming state to armed, **D** = transition from normal to short to normal changes arming state to disarmed, **I** = instant alarm, **T** = trouble, **blank** = no response																	

The point response is fixed to 1 for the Keyswitch Momentary Point type. Changing the point circuit state from normal to short to normal, toggles the armed state of the area. If the area is armed (All On, Part On) it is disarmed (Off). If the area is disarmed it is armed (All On). An open on the point circuit creates a point trouble while the area is disarmed (Off). An open on the point circuit while the area is armed (All On, Part On) creates an instant alarm. When the point circuit returns from open to normal the trouble restores.

Open/Close Point Type, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open		I														
Armed	Short		D														
Disarmed	Open		T														
Disarmed	Short		D														
Key: D = transition from normal to short changes point arming state to disarmed (point arming state is armed when point circuit state is normal), **I** = instant alarm, **T** = trouble, **blank** = no response																	

The point response is fixed to 1 for the Open/Close Point type.
Changing the point circuit state to normal arms the point. The control panel sends a point closing report. Changing the circuit state from normal to open creates an instant point alarm.
Changing the point circuit state to short disarms the point. The control panel sends a point closing report. Changing the circuit state from short to open creates a point trouble.

Custom Function Point Type, Single EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open							CF	CF	T	CF		CF	CF	T	CF	
Armed	Short						CF		CF	CF	T	CF		CF	CF	T	
Disarmed	Open		CF	CF	T	CF		CF	CF	T	CF						
Disarmed	Short	CF		CF	CF	T	CF		CF	CF	T						
Key: CF = control panel executes custom function on transition to circuit state. **T** = trouble, **blank** = no response																	

When the point circuit state changes the control panel responds by starting a custom function.

Custom Function Point Type, Dual EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short						T	T	T	T	T	T	T	T	T	T	
Armed	Fault		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Disarmed	Open/ Short						T	T	T	T	T	T	T	T	T	T	
Disarmed	Fault		CF	T	CF		CF	CF	CF	T	CF	CF	CF	CF	CF	T	
Key: CF = control panel executes custom function on transition to circuit state. **T** = trouble, **blank** = no response																	

When the point circuit state changes the control panel responds by starting a custom function.

Custom Function Point Type, Single EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	TA	TA	TA	TA	TA	CF	T	CF	CF							
Armed	Short	CF	T	CF	CF		TA	TA	TA	TA	TA						
Disarmed	Open	TA	TA	TA	TA	TA	CF	CF	T		CF						
Disarmed	Short	CF	CF	T		CF	TA	TA	TA	TA	TA						
Key: CF = control panel executes custom function on transition to circuit state. **T** = trouble, **TA** = tamper alarm, **blank** = no response																	

When the point circuit state changes the control panel responds by starting a custom function.

Custom Function Point Type, Dual EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	TA	TA	TA	TA	TA											
Armed	Fault	CF		CF	T	CF											
Disarmed	Open/ Short	TA	TA	TA	TA	TA											
Disarmed	Fault		CF	CF	CF	T											
Key: CF = control panel executes custom function on transition to circuit state. **T** = trouble, **TA** = tamper alarm, **blank** = no response																	

When the point circuit state changes the control panel responds by starting a custom function.

Notice!
Control panel firmware requirements for Single EOL with Tamper and Dual EOL with Tamper circuit styles.
To use a Single EOL with Tamper or Dual EOL with Tamper circuit style, make sure the control panel firmware is v3.06 or greater.

Notice!
For Dual EOL Circuit Style, purchase second 1kΩ **EOL separately**
Order ICP-1K22AWG-10, package of 10 resistors.

Notice!
For Dual EOL Circuit Styles, circuit states are normal, fault, short, open
Normal - the N/C (normally closed) switch shown in the circuit diagram is closed.
Fault - the N/C switch shown in the circuit diagram is open.
Short - the sensor loop is shorted.
Open - the sensor loop circuit is open.

Notice!
Control panel and B208 Octo-input firmware requirements for Dual EOL
To use the Dual EOL Circuit style, verify the control panel firmware is v3.01 or greater.
If you are using a B208 Octo-input Module, verify the module firmware is v2.1.1 or greater.

Custom Function Point Type, No EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Fault		T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Disarmed	Fault		CF	T	CF		CF	CF	CF	CF	CF	CF	CF	CF	CF	T	
Key: CF = control panel executes custom function on transition to circuit state. **T** = trouble, **blank** = no response																	

When the point circuit state changes the control panel responds by activating a custom function.

Notice!
For the No EOL Circuit Style, circuit states are normal and fault, in the Point Diagnostic window, circuit status is open or short
In the point response tables, the circuit states are normal and fault for the No EOL Circuit Style. The *Normal State, page 218* parameter defines the normal and fault circuit states.
For No EOL circuit style points, the point diagnostics window shows open or short in the circuit status column.

Water, High Temp, Low Temp Point Types, No EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Fault	I	T														
Disarmed	Fault	I	T														
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Water, High Temp, Low Temp Point Types, Single EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	I	T	I	T			I	T								
Armed	Short	I	I	T	T	I	T										
Disarmed	Open	I	T	I	T			I	T								
Disarmed	Short	I	I	T	T	I	T										
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Water, High Temp, Low Temp Point Types, Dual EOL Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	T	I	T	I												
Armed	Fault	I	I	T	T												
Disarmed	Open/ Short	T	I	T	I												
Disarmed	Fault	I	I	T	T												
Key: I = instant alarm, **S** = supervisory alarm, **T** = trouble, **blank** = no response																	

Water, High Temp, Low Temp Point Types, Single EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open	TA	TA	TA	I	T			I	T							
Armed	Short	I	T	TA	TA	TA	I	T									
Disarmed	Open	TA	TA	TA	I	T			I	T							
Disarmed	Short	I	T	TA	TA	TA	I	T									
Key: I = instant alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Water, High Temp, Low Temp Point Types, Dual EOL with Tamper Circuit Style, Point Response Selections																	
Armed State	**Circuit State**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Armed	Open/ Short	TA	TA	TA	TA												
Armed	Fault	I	T	TA													
Disarmed	Open/ Short	TA	TA	TA	TA												
Disarmed	Fault	I	T	TA													
Key: I = instant alarm, **T** = trouble, **TA** = Tamper Alarm, **blank** = no response																	

Notice!
Supervisory and tamper alarms for Environmental points
For Environmental points, Supervisory and Tamper Alarm responses are interpreted as Trouble point responses.

Point Response for B820 SDI2 Inovonics Interface Module
When the point Source parameter is set to Wireless and the Wireless Module Type parameter is set to B820 Inovonics Wireless, wireless points:
- send Short for point fault (regardless of sensor loop open/short state)
- send Open for a tamper event (enclosure cover removed)

Point Response for B810 RADION receiver SD
When point Source is set to wireless and the Wireless Module Type parameter is set to B810 RADION Wireless, wireless points:
- send Open or Short for point fault (the electrical state of the sensor loop)
- send Short for the reed switch (magnet not present)
- send Tamper for a tamper event (enclosure cover removed)

RPS Menu Location
Points > Point Indexes > Point Type / Response / Circuit Style

Further information
Point Type, page 190
Circuit Style, page 205
Normal State, page 218

11.3.7 Circuit Style

Default: Single EOL (1KΩ)
Selections:
- Single EOL (1KΩ)
- Single EOL (2KΩ)
- Dual EOL (1KΩ)
- No EOL
- Single EOL (1KΩ) with Tamper
- Single EOL (2KΩ) with Tamper
- Dual EOL (1KΩ) with Tamper

Select the circuit style and end of line resistor for the point sensor loop.
The Single EOL (1KΩ) selection is valid for all point sources.
The Single EOL (1KΩ) with Tamper selection is only valid for Octo-input (B208), Onboard, Output, Keypad, IP Camera, and Door point sources.
The Single EOL (2KΩ), Single EOL (2KΩ) with Tamper, Dual EOL (1KΩ), Dual EOL (1KΩ) with Tamper, and No EOL selections are only valid for On-board and Octo-input (B208) point sources.

Notice!
EOL resistors for ZONEX, Wireless, POPEX point devices
When the POINTS > Point Assignments > Source parameter is set to ZONEX, Wireless, or POPEX, set Circuit Style to Single EOL (1KΩ).
Even though the Circuit Style is set to Single EOL (1KΩ), **do not** replace the EOL resistors supplied with ZONEX, POPEX, or wireless point devices with 1KΩ EOL resistors.

Notice!
Circuit Style control panel firmware requirements
The Circuit Style Parameter is not available for control panel firmware v2.xx.
The Dual EOL (1KΩ) resistor selection is for control panel firmware v3.01 and higher.
The Single EOL (2KΩ) and No EOL selections are for control panel firmware v3.03 and higher.
The Single EOL (1KΩ) with Tamper, Single EOL (2KΩ) with Tamper, and Dual EOL (1KΩ) with Tamper selections are for control panel firmware v3.06 and higher.

RPS Menu Location
Points > Point Profiles > Point Type/Response/Circuit Style

Further information
Point Type, page 190
Point Response, page 195

11.3.8 Entry Delay

Default: 30 seconds
Selections: 5 - 600 seconds (5-second increments)
Enter the number of seconds of entry delay time. Entry delay time gives users time to disarm before the control panel makes an alarm event.
If Entry Delay time ends before the user disarms, the control panel creates an alarm event.
Entry delay begins when a user faults a point with the *Point Type, page 190* parameter set to Part On, Interior, or Interior Follower, and the *Point Response, page 195* parameter set to 4, 5, 6, 7, or 8.
If another delay point is faulted 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 left.

Notice!
UL requirement
To comply with UL standards, the total amount of time entered in Entry Delay and *Alarm Abort, page 215* must not exceed 1 minute.

Notice!
SIA CP-01 False Alarm Reduction requirement
To comply with SIA CP-01 False Alarm Reduction, set this parameter between 30 and 240 seconds for all point profiles. Refer to SIA CP-01 Verification for more information.

RPS Menu Location
Points > Point Profiles > Entry Delay

11.3.9 Entry Tone Off

Default: No (for all Point Profiles)
Selections:
– Yes - entry tone does not start when this point starts entry delay.
– No - entry tone starts when this point starts entry delay.
Do not set this parameter to Yes for points used to tell the user to disarm after entering the premises.
To suppress the entry tone per keypad, set the Keypads > Keypad Assignments > *Entry Tone, page 118* parameter to No.

RPS Menu Location
Points > Point Profiles > Entry Tone Off

11.3.10 Silent Bell

Default:
- Point Profile 2 - Yes
- All other Point Profiles - No

Selections:
- Yes - Activate the Silent Alarm output when this point goes into alarm. Do not activate the Alarm Bell output or keypad alarm sounders. This parameter has no effect on Fire and Gas points.
- No - Do not activate the Silent Alarm output when this point goes into alarm.

Notice!
Alarm Bell activates after two failed attempts to central station receiver
If you set the *Audible After Two Fails, page 207* parameter to Yes, the *Alarm Bell, page 135* activates after two failed attempts to send a Silent Alarm report to the central station receiver.

RPS Menu Location
Points > Point Profiles > Silent Bell

11.3.11 Tamper Response

Default: Always Alarm

Selections:
- Always Alarm - point tamper alarms are always audible and visible (default).
- Alarm while Disarmed - point tamper alarms are silent and invisible while the point's area is armed (CHI panel default).

RPS Menu Location
Points > Point Profiles > Point Tamper Option

11.3.12 Ring Until Restored

Default: No (for all Point Profiles)

Selections:
- Yes - Fire Bell or Gas Bell outputs (and keypad sounders) cannot be silenced until the point is restored to normal. If the point restores and the alarm is not silenced, the output continues until Fire time or Gas time expires. If the point does not restore, the output continues even after Fire time or Gas time expires.
- No - Fire Bell or Gas Bell outputs (and keypad alarm sounders) can be silenced whether or not the point is restored to normal. If the Fire Bell or Gas Bell is not silenced, the output continues until Fire time or Gas time expires.

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

RPS Menu Location
Points > Point Profiles > Ring Until Restored

11.3.13 Audible After Two Fails

Default: No (for all Point Profiles)

Selections:

– Yes - for silent points (Silent Bell parameter set to Yes), the Alarm Bell output activates after two failed attempts to send a report to the central station receiver.
– No - for silent points (Silent Bell parameter set to Yes), the Alarm Bell output does not activate after two failed attempts to send a report to the central station receiver.

When a silent point (*Silent Bell, page 207* parameter set to Yes) is faulted, Burg Time starts immediately. It could take up to 3 minutes before the second attempt to send a report to the central stations receiver fails. Make sure the *Burg Time, page 103* parameter is set to include these 3 minutes plus the number of minutes you want the *Alarm Bell, page 135* output to activate.

RPS Menu Location
Points > Point Profiles > Audible After 2 Fails

11.3.14 Invisible Point

Default:
– Yes - Point Profile 2
– No - All other Point Profiles

Selections:
– Yes - keypads do not show alarm events for this point. Keypads make the alarm tone, show trouble events and make the trouble tone.
– No - keypads show alarm events and trouble events. Keypads make the alarm tone and the trouble tone for this point.

Notice!
Fire, gas, environmental points do not apply
The invisible point parameter does not apply to fire, gas or environmental (water, high temp, low temp) points.

To prevent the keypad alarm tone and the *Alarm Bell, page 135* from sounding, set the *Silent Bell, page 207* parameter to Yes.

RPS Menu Location
Points > Point Profiles > Invisible Point

11.3.15 Buzz on Fault

Default:
– 1- Point Profile 9
– 0 - All other Point Profiles

Selections:
0 - Buzz on Fault is disabled, trouble tone only if point is in trouble state.
1 - the trouble tone starts when the point is faulted. The trouble tone cannot be silenced until the point is restored to the normal state.
2 - the trouble tone starts when the point is faulted. The trouble tone can be silenced before the point restores to the normal state.
3 - the trouble tone starts when the point is faulted. The trouble tone automatically stops when the point restores to the normal state. The trouble tone cannot be silenced when the point is faulted.
Instant Alarm (I), Trouble (T) and Supervisory (S) point responses take priority over Buzz on Fault. If the Point Response parameter is "blank", only the Buzz on Fault starts the trouble tone. Refer to the *Point Response, page 195* parameters for a description of response types for each point type and how they are affected by the armed state.

If an alarm, trouble, or supervisory event occurs and is acknowledged, Buzz on Fault selections 1 and 3 continue the trouble tone until the point restores to the normal.

Notice!
This Buzz on Fault parameter does not apply to the Custom Function point type.

Notice!
UL 985 requirement for Household Fire Warning System Units
Set this parameter to 1 (The trouble tone starts when the point is faulted and the tone cannot be silenced until the point is restored to the normal state) to comply with UL 985 requirements.

RPS Menu Location
Points > Point Profiles > Buzz on Fault

11.3.16 Watch Point

Default:
- Yes - Point Profiles 7 to 8
- No - All other Point Profiles

Selections:
- Yes - when the control panel is in watch mode, this point starts the watch tone when it is faulted.
- No - this point does not start the watch tone when it is faulted.

The Watch Tone sounds for 2 seconds and the point name shows in the keypad display on keypads assigned to the same area as the point.
Watch Points are active when the Point Response is blank (no response). The Point Type must be 24 Hour, Part On, or Interior.

RPS Menu Location
Points > Point Profiles > Watch Point

11.3.17 Output Response Type

Default: 0

Selections:
- 0- disabled, the point state does not affect the operation of the related output.
- 1- changing this point to any off normal point state activates the related output. The output automatically resets when the point returns to the normal state.
- 2- when this point goes into alarm, the related output latches. The output remains latched until the alarm event is cleared from the keypad.

Use this parameter to configure outputs to activate in a steady pattern when a related point (point with the same number as the output, point 8 and output 8 for example) changes to an off normal point state.
Set this parameter to 0 when the related output is configured for any other output function.

Output Follows Point
Use Outputs to activate when a point programmed for Output Response Type is Off Normal or In Alarm event.

RPS Menu Location
Points > Point Profiles > Output Response Type

11.3.18 Display as Device

Default: No

Selections:

– Yes - show [CHECK DEVICE] at keypads when this point is off normal.

– No - do not show [CHECK DEVICE] when this point is off normal.

Use this feature for points that are connected to a trouble output of a device.

RPS Menu Location

Points > Point Profiles > Display as Device

11.3.19 Local While Disarmed

Default:

– Yes - Point Profile 9, 12

– No - All other Point Profiles

Selections:

– Yes - while the area is disarmed, the control panel does not send alarm, trouble, or restoral reports for this point.

– No - the control panels sends alarm, trouble, and restoral reports for this point while the area is disarmed.

This parameter has no effect on fire points or gas points.

Do not set this parameter to Yes for Keyswitch Maintained, Keyswitch Momentary, or Open/Close point types.

Do not set this parameter to Yes for 24 hour points. 24 hour points are always armed. Instead, choose a controlled point type and use a point response that sends an alarm whether the point is armed or not. For example, points with the *Point Type, page 190* parameter set to Part On and the *Point Response, page 195* parameter to 9 send an alarm on a trouble or a short (I) whether the area is armed or not.

Notice!

A restoral report is sent 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.

RPS Menu Location

Points > Point Profiles > Local While Disarmed

11.3.20 Local While Armed

Default: No

Selections:

– Yes - while the area is armed, the control panel does not send alarm, trouble, or restoral reports for this point.

– No - the control panels sends alarm, trouble, and restoral reports for this point while the area is armed.

This parameter has no effect on fire points or gas points.

Do not set this parameter to Yes for Keyswitch Maintained, Keyswitch Momentary, or Open/Close point types.

Do not set this parameter to yes for 24 hour points. 24 hour points are always armed. Instead, choose a controlled point type and use a point response that sends an alarm whether the point is armed or not. For example, points with the *Point Type, page 190* parameter set to Part On and the *Point Response, page 195* parameter to 9 send an alarm on a trouble or a short (I) whether the area is armed or not.

RPS Menu Location
Points > Point Profiles > Local While Armed

11.3.21 Disable Restorals

Default: No
Selections:
– Yes - disable restoral reports for this point.
– No - enable restoral reports for this point.

RPS Menu Location
Points > Point Profiles > Disable Restorals

11.3.22 Force Arm Returnable

Default: No
Selections:
– Yes - when this point returns to the normal state after being force armed (forced point bypass), it automatically goes to the armed state.
– No - when this point returns to the normal state after being force armed (forced point bypass), it stays force bypassed.

Set this parameter to Yes for points that are typically faulted when arming the area. when this point returns to the normal state after being force armed (forced point bypass), it automatically goes to the armed state with the other points in the area.

RPS Menu Location
Points > Point Profiles > Force Arm Returnable

11.3.23 Bypass Returnable

Default: No
Selections:
– Yes - controlled points that are bypassed or swinger bypassed automatically unbypass when the area is disarmed.
– No - controlled points that are bypassed or swinger bypassed must be unbypassed. Use the UNBYPASS? keypad function, the Unbypass a Point or the Unbypass All Points SKED functions, or RPS to unbypass.

Set this parameter to No for interlock points.
Controlled points that are force armed (bypassed) are always unbypassed when the area is disarmed.

RPS Menu Location
Points > Point Profiles > Bypass Returnable

11.3.24 Bypassable

Default:
– Yes - Point Profiles 1, 7-13, 20
– No - Point Profiles 2-6, 14-19

Selections:
– Yes - points assigned to this profile can be bypassed and force armed.
– No - points assigned to this profile cannot be bypassed or force armed.

Even when this parameter is set to No:
– Faulted controlled points are force armed at the end of the close window when the Auto Close parameter is set to Yes.
– Faulted controlled points are force armed when the area is armed by a Sked.

When a 24-hour point or environmental point is bypassed, 24 HOUR BYPASS scrolls on the keypad. FIRE BYPASS scrolls for bypassed fire points. GAS BYPASS scrolls for bypassed gas points.
For 24 hour alarm response without the continuous scrolling of a bypassed 24-hour point, use a Part On point with a *Point Response, page 195* of 9 to E.

RPS Menu Location
Points > Point Profiles > Bypassable

11.3.25 Swinger Bypass

Default: No
Selections:
– Yes - enable Swinger Bypass for this point. The control panel automatically bypasses the point when the number of point alarm or point trouble events reaches the Swinger Bypass Count.
– No - disable Swinger Bypass for this point.

With each point alarm or point trouble event the control panel adds 1 to the event count. When the area is disarmed the control panel resets the event count to 0.
The control panel sends Swinger Bypass reports when the *Swinger Bypass Count, page 84* is reached and *Report Bypass at Occurrence, page 212* is set to Yes.
The *Bypassable, page 211* parameter does not need to be set to Yes for swinger bypass to work.
If the *Bypass Returnable, page 211* parameter is set to Yes, swinger bypassed points are automatically unbypassed when the area is disarmed.

RPS Menu Location
Points > Point Profiles > Swinger Bypass

11.3.26 Report Bypass at Occurrence

Default: No
Selections:
– Yes - the control panel sends a bypass report at the time that the point is bypassed.
– No - the control panel does not send a bypass 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 by using the *Defer Bypass Report, page 212*.

RPS Menu Location
Points > Point Profiles > Report Bypass at Occurrence

11.3.27 Defer Bypass Report

Default: No
Selections:
– Yes - the control panel sends Bypass Reports with the closing report instead of when the point is bypassed by a user.
– No - the control panel does not send 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 and any point being bypassed during the arming sequence report as POINT BYPASS 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, page 212* are both set to No.

RPS Menu Location
Points > Point Profiles > Defer Bypass Report

Refer to
– *Report Bypass at Occurrence, page 212*

11.3.28 Cross Point

Default: No
Selections:
– Yes - this point is a Cross Point.
– No - this point is not a Cross Point.

The Cross Point option reduces false alarms. Points can be programmed so that the control panel requires an Alarm condition within a programmed period of time (Cross Point Time) from at least two points within a Cross Point Group before Cross Point Alarm Events are generated.
A fault on a Cross Point starts the Cross Point Timer on the control panel. If there is a fault on another Cross Point in the same Cross Point Group before the Cross Point Timer expires, the control panel makes Cross Point Alarm events for both points.
If the Cross Point that starts the Cross Point Timer restores to normal and there is no fault on another Cross Point in the same Cross Point Group before the Cross Point Timer expires, the control makes an unverified event (not a Cross Point Alarm Event).
If the Cross Point that starts the Cross Point Timer restores to normal, then is faulted and restores again, and there is no fault on another Cross Point in the same Cross Point Group before the Cross Point Timer expires, the control makes an unverified event (not a Cross Point Alarm Event).
If the Cross Point that starts the Cross Point Timer remains faulted until the Cross Point Timer expires and there is no fault on another Cross Point in the same Cross Point Group, the control panel makes a Point Alarm Event (not a Cross Point Alarm Event).
The Cross Point function applies only to alarm events. It does not apply to supervisory or trouble events.
The Cross Point function requires that at least 2 points in the group be Cross Points.
Cross Point Groups cannot be configured. There are 8 points in each Cross Point Group. Points 1-8 are the first group. Points 9-16 are the second group, and so on. Cross points in different Cross Point Groups do not affect each other.
Assign Cross Points in the same Cross Point Group to the same Point Profile:
1. Set the *Point Type, page 190* parameter. Use a valid parameter from the list in the next section of this topic.
2. Set the *Point Response, page 195* parameter for instant alarm response.

If you assign Cross Points in the same Cross Point Group to different Point Profiles and you want to use the Alarm Abort feature, set the *Alarm Abort, page 215* parameter to Yes for each Point Profile.

Setting the *Bypassable, page 211* parameter to Yes for Cross Points can prevent Cross Point alarms. For example, if points 1 and 2 are Cross Points, point 1 is bypassed, and point 2 is faulted, the control panel can not create a Cross Point event. If point 2 remains faulted until the Cross Point Timer expires, the control panel makes a Point Alarm Event (not a Cross Point Alarm Event). If point 2 is faulted and restores before the Cross Point Timer expires, when the timer expires the control panel makes an unverified point event (not a Cross Point Alarm Event).

Supported Point Type parameters

- 24 hour
- Interior
- Interior follower
- Part On
- High Temp
- Low Temp
- Water

RPS Menu Location

Points > Point Profiles > Cross Point

Further information

Cross Point Timer, page 188

11.3.29 Alarm Verify

Default:

- Yes - Point Profile 5
- No - All other Point Profiles

Selections:

- Yes - Enable alarm verification for this point. (Fire and Gas point types only)
- No - Disable alarm verification on this point.

If you set this parameter to Yes, you must also set the Resettable parameter to Yes.
When a Fire or Gas point with Alarm Verity set to Yes goes into alarm, the control panel starts the Reset Sensors output function to remove power to resettable points. When power comes back on, the control ignores the point for the time set in the Restart Time parameter. If the point is in alarm within 65 seconds of the end of restart time, the control panel creates an alarm event.
The control panel does not use the time set in the Restart Time parameter for the Fire Walk Test. The restart time is 5 seconds.

RPS Menu Location

Points > Point Profiles > Alarm Verify

Further information

Restart Time, page 98
Resettable, page 214
Reset Sensors, page 136

11.3.30 Resettable

Default:

- No - Point Profiles 1-3, 6-20
- Yes - Point Profiles 4,5

Selections:

– Yes - the control panel ignores this point for the reset time in the Reset Sensors user function and the reset/restart time in alarm verification function.
– No - This point is not resettable.

The Resettable parameter is for 24-hr, Part On, Interior, Panic, Fire, and Gas point types only.

Set this parameter to Yes for points that require interruption of power to reset a latched alarm event. The resettable point function is typically used for smoke detectors and glass break detectors. Do not mix fire and intrusion devices on the same powered loop.

When points are reset using the Reset Sensor user function, a walk test, or RPS the control panel sends a sensor reset report to the central station receiver.

Further information

Alarm Verify, page 214
Restart Time, page 98
Reset Sensors, page 136

RPS Menu Location

Points > Point Profiles > Resettable

11.3.31 Alarm Abort

Default:

– Yes - Point Profiles 1, 7-10, 11-16, 20
– No - Point Profiles 2-6, 17-19

Selections:

– Yes - if the point goes into alarm, the control panel delays the alarm report for the time set in the Abort Window parameter.
– No - the control panel does not delay alarm reports.

If a user silences the alarm before the time in the Abort Window ends, the alarm is aborted. The point alarm report is not sent to the central station receiver.

When an alarm is aborted, keypads can show an Alarm Not Sent message. Refer to *Abort Display, page 119*.

This parameter does not apply to fire alarms or invisible point alarms.

Notice!

To comply with UL standards, the total amount of time entered in the *Entry Delay, page 206* parameter and the *Abort Window, page 83* parameter must not exceed 1 minute.

RPS Menu Location

Points > Point Profiles > Alarm Abort

11.3.32 Wireless Point Supervision Time

Default:

– 24 Hours - Point Profiles 1-2, 7-16
– 4 Hours - Point Profiles 3-6

Selections:

– None - Disable wireless point supervision.
– 4 Hours, 12 Hours, 24 Hours, 48 Hours, 72 Hours - set the time in hours for wireless point supervision.

If the wireless receiver does not receive a transmission from the wireless point device within the Wireless Point Supervision Time, the control panel makes a missing event for the point.

The Wireless Point Supervision Time parameter for fire points is set to 4 hours and cannot be edited.
Wireless Point Supervision Time applies to RADION keyfobs when they are configured as a point devices.
This is an alternate supervision interval to the global *System (Repeater) Supervision Time, page 267* setting.

RPS Menu Location
Points > Point Profiles > Wireless Point Supervision Time

11.3.33 Custom Function

Default: Disabled
Selections:
- B6512 - Disabled, Function 128-133
- B5512 - Disabled, Function 128-131
- B4512 - Disabled, Function 128-129
- B3512 - Disabled, Function 128

Select the custom function to start when the point is faulted to the short (S) or open (O) state.

RPS Menu Location
Points > Point Profiles > Custom Function

11.3.34 Monitor Delay

Default: 00:00
Selections: 00:00 (disabled), 00:01-60:00
Set the time (MM:SS) a disarmed control panel waits after a point faults before sending a Burg Supervisory report to the central station. The point must be faulted the entire time. If the point restores to normal during this time, no report is sent.
The control panel does not show monitor delay events at keypads.
Use the Monitor Delay feature to monitor doors that should not be left open. For example, trash compactor doors, jewelry case door, and freezer doors.

Notice!
Starting a walk test that includes controlled points, or arming the points' area cancels the monitor point timer. No report is sent after the configured time expires.

RPS Menu Location
Points > Point Profiles > Monitor Delay

11.3.35 Delay Response, Disarmed

Default: 00:00
Selections: 00:00 (disabled), 00:05-60:00
This parameter sets the length of time (MM:SS) the control panel waits after a disarmed point faults before annunciating or reporting the fault.

Notice!
Panic points profiles
This parameter is not configurable (disabled) for Panic, Water, High Temp and Low Temp Point Profiles.

This parameter only applies to the following point types when disarmed:
- *Part On, page 218*
- *Interior, page 219*
- *Interior Follower, page 219*

Use this feature to delay the effect of the following parameters:
- *Point Response, page 195*
  - Instant Alarm
  - Supervisory
- *Buzz on Fault, page 208*
- *Watch Point, page 209*
- *Output Response Type, page 209*
- *Display as Device, page 210*
- *Output, page 185*

Notice!
Point Response (D) Delay Alarm is not supported by Delay Response feature. So, when a Delay Alarm results in an instant alarm, that alarm is not delayed by this feature.

RPS Menu Location
Points > Point Profiles > Delay Response Disarmed

11.3.36 Delay Response, Armed

Default: 00:00
Selections: 00:00 (disabled), 00:05-60:00
This parameter sets the length of time (MM:SS) the control panel waits after an armed point faults before annunciating or reporting the fault.

Notice!
Panic point profiles
This parameter is configurable (enabled) for Panic, Water, High Temp, and Low Temp Point Profiles.

This parameter only applies to the following point types when armed:
- *24-Hour, page 218*
- *Part On, page 218*
- *Interior, page 219*
- *Interior Follower, page 219*
- *Panic Point, page 222*
- *Water Point, page 221*
- *High Temp Point, page 221*
- *Low Temp Point, page 221*

Use this feature to delay the effect of the following parameters:
- *Point Response, page 195*
  - Instant Alarm
  - Supervisory
- *Output Response Type, page 209*
- *Display as Device, page 210*
- *Output, page 185*

Notice!
Point Response (D) Delay Alarm is not supported by Delay Response feature. So, when a Delay Alarm results in an instant alarm, that alarm is not delayed by this feature.

RPS Menu Location
Points > Point Profiles > Delay Response Armed

11.3.37 Normal State

Default: Open
Selections:
– Open - an open point circuit is the Normal state.
– Short - a short on point circuit is the Normal state.
This parameter sets the Normal state when the Circuit Style parameter is set to No EOL.

RPS Menu Location
Points > Point Profiles > Point Type/Response/Circuit Style

11.4 Point Profile descriptions

11.4.1 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, page 208*.
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, page 195* 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, page 210* 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”.

11.4.2 Part On

Configuring a point profile with the Part On point type makes it a Part On point profile. Points assigned to a Part On point profile are Point On points. Part On points are typically used to monitor devices in the perimeter of the premises (doors and windows).
A Part On point profile includes a configurable entry delay time. Entry delay time provides time for users to reach a keypad and turn the area Off without creating an alarm event. For example, when a user opens the front door (tripping a Part On point) entry delay time begins. The user needs to proceed to a keypad and turn the area off before exit delay time expires to prevent an alarm event.
If the area is in entry delay and a second Part On point trips, the control panel compares the remaining entry delay time to the entry delay time programmed for the second Part On point. If the second point's entry delay time is less than the remaining time, it shortens the entry delay time.

Notice!

Part On Points with instant Point Response create immediate alarm events

Perimeter Points programmed for an instant *Point Response, page 195* do not start entry delay time when tripped. They generate an alarm event immediately, even during entry or exit delay.

When a user turns an area All On; Part On points, Interior points, and Interior Follower points are all armed.

When a user turns an area Part On only Part On points are armed. Interior points, and Interior Follower points are not armed. In a typical system, turning an area Part On arms only the perimeter protection allowing users to remain in the premises without creating alarm events from interior points.

11.4.3 Interior

Configuring a point profile with the Interior point type makes it an Interior point profile. Points assigned to an Interior point profile are Interior points. Interior points are typically used to monitor interior detection devices such as interior doors, motion detectors, photoelectric beams, or carpet mats.

Interior points are armed only when the area is All On. They are not armed when the area is Part On.

The *Point Response, page 195* for Interior points can be configured for instant or delayed alarm response.

- Instant - points configured for instant alarm response create alarm events immediately, even during entry or exit delay time. Interior points are commonly configured for instant alarm response.
- Delayed - when an interior point configured for delayed alarm response is tripped while the area is All On, it initiates entry delay time. It will not create an alarm event unless entry delay time expires before the area is turned off.

  If the area is already in entry delay when an interior point with delayed alarm response trips, the control panel compares the remaining entry delay time to the entry delay 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, page 206*).

Notice!

Use the *Interior Follower, page 219* **profile for instant alarm if the area is not in entry delay**

For some installations you may want an interior point that follows, but can not initiate entry day. Tripping an Interior Follower point while the area is All On creates an instant alarm event. However, if another point is tripped starting entry delay, and then the Interior Follower point is tripped, the Interior Follower point delays the alarm response until exit delay time expires. If the area is turned Off before entry delay time expires there is no alarm response.

11.4.4 Interior Follower

Configuring a point profile with the Interior Follower point type makes it an Interior Follower point profile. Points assigned to an Interior Follower point profile are Interior Follower points. Interior Follower points are typically used to monitor interior detection devices such as interior doors, motion detectors, photoelectric beams, or carpet mats.

Interior Follower points are armed only when the area is All On. They are not armed when the area is Part On.
Interior Follower points follow, but can not initiate entry delay. Tripping an Interior Follower point while the area is All On creates an instant alarm response. However, if another point is tripped starting entry delay, and then the Interior Follower point is tripped, the Interior Follower point delays the alarm response until exit delay time expires. If the area is turned Off before entry delay time expires there is no alarm response
During Exit Delay, faulting an Interior Follower point does not create an alarm event (even if a Part On, Delay point is not faulted during the exit delay).
Interior Follower points do not initiate entry delay even when configured for a delayed alarm response (*Point Response, page 195* set to 4, 5, 6, 7, or 8).

Notice!
Use the *Interior, page 219* **profile and delayed alarm response for interior points that initiate entry delay**
For some installations you may want an interior point that can initiate entry day. Tripping an Interior point configured for delayed alarm response (refer to *Point Response, page 195*) while the area is All On initiates entry delay. The alarm response is delayed until exit delay time expires. If the area is turned Off before entry delay time expires there is no alarm response.

11.4.5 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 While Disarmed, page 210* is set to Yes.
Alarm and restoral reports are not sent if *Local While Armed, page 210* is set to Yes.

Notice!
Point Response 2 is required for Inovonics FA113 Wireless devices.

11.4.6 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 While Disarmed, page 210* is set to Yes.
Trouble and restoral reports are not sent if *Local While Armed, page 210* is set to Yes.

11.4.7 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 While Armed, page 210* 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 While Disarmed, page 210* 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.

11.4.8 Fire Point

This point type generates a Fire Alarm. Fire alarms are the highest priority event in the control panel.

11.4.9 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, page 195*; therefore, no alarm event occurs.
If this point type is bypassed, 24 HOUR PT BYPASSED is shown on the keypads.

11.4.10 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).

11.4.11 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.

11.4.12 Water Point

Use this Environmental Point Type to monitor water sensors that can detect a water leak. An instant alarm or trouble point response is reported as a water leakage event. Environmental point types are uncontrolled.

11.4.13 High Temp Point

Use this Environmental Point Type to monitor high temperatures. An instant alarm or trouble point response is reported as a temperature event. Environmental point types are uncontrolled.

11.4.14 Low Temp Point

Use this Environmental Point Type to monitor low temperatures. An instant alarm or trouble point response is reported as a temperature event. Environmental point types are uncontrolled.

11.4.15 Panic Point

The Panic Point Type operates the same as a 24 Hour point type and can be programmed with or without audible output. This point type is armed at all times and is used for panic alarms.

12 Schedules

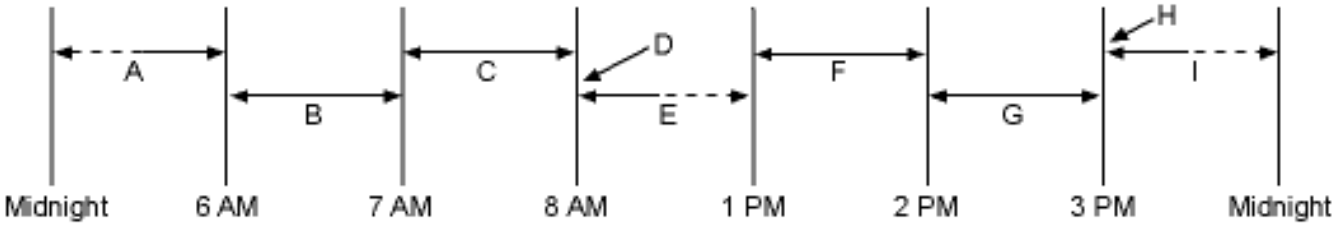
12.1 Open/Close Windows

Use these windows to set schedules for disarming (open) and arming (close). Opening and closing windows 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.
The disarming and arming schedules provide several independent features:

- Suppress normal opening and/or closing reports when *Disable O/C in Window, page 106* is set to Yes.
- Generate a FAIL TO OPEN report if the area is not disarmed on schedule when *Fail to Open, page 107* 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, page 107* is set to Yes.
- Automatically arm the area at the end of the closing window when *Auto Close, page 107* is set to Yes.

12.1.1 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 the week	Early begin	Start	Stop	Early begin	Start	Stop	Except on Holiday
1	S**MTWT F**S	06:00	07:00	08:00			23:59	Yes / **No**
2	S**MTWT F**S	13:00	14:00	15:00			01:00	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#	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**	1234	**1**23456 78
2 / Monday	00:00	00:00	00:30				Yes / **No**	1234	**1**23456 78

12.1.2 Opening_Closing windows table

Monday to Friday, opening between 5 and 6 AM, closing between 11 PM and 1 AM.

		Open			**Close**			
W#	Day of the week	Early begin	Start	Stop	Early begin	Start	Stop	Except on Holiday
1	S**MTWT F**S	04:00	05:00	06:00	20:00	23:00	23:59	Yes / **No**
2	SM**TWT 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	SMTWTFS	07:00	08:00	08:30

		Open
	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	Days(s) of the week	NO	None	Program at least on 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 on 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 on area as YES
All days must be programmed NO	Only on holidays	NO	Select at least one Index	Program at least on area as YES

12.1.3 Sunday through Saturday

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, page 231* to Yes, and enable at least one holiday index. When *Xept Holiday, page 231* 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, page 231* 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

12.1.4 Open Early Begin

Default: Disable

Selections: Disable, HH:MM (hours and minutes) 00:00 to 23:59

Enter the earliest time that a user is allowed to open (disarm) an area.

This parameter is one of three required to create an opening window. To finish programming an opening window, *Open Window Start, page 226* and *Open Window Stop, page 227* 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, page 226* 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, page 106* 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, page 106* 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

12.1.5 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.

Further information
Close Early Begin, page 227
Open Window Stop, page 227

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

12.1.6 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, *Close Early Begin, page 227* and *Open Window Start, page 226* must also be programmed.
If the area is not disarmed by the time the *Open Window Stop, page 227* time expires, the control panel generates a FAIL TO OPEN report if enabled in *Fail to Open, page 107*.
Opening reports generated between the Open Window Start time and Open Window Stop time can be suppressed by setting *Disable O/C in Window, page 106* 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.
The control panel does not send FAIL TO OPEN reports for windows that stop at 23:59.

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

12.1.7 Close Early Begin

Default: Disable
Selections: Disable, HH:MM (hours and minutes) 00:00 to 23:59
Enter the earliest time the user can close an area before the Close Window Start time.
This parameter is one of three required to create a closing window. To finish programming a closing window, *Close Window Start, page 228* and *Close Window Stop, page 228* 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, page 106* 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, page 226* time that is between another window's *Open Window Start, page 226* and *Open Window Stop, page 227* 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

12.1.8 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, page 227* and *Close Window Stop, page 228* 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, page 227* for report feature explanations.

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

12.1.9 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	**SMTWT** FS				22:00	23:30	23:59	Yes / **No**
2	S**MTWT F**S				00:00	00:00	00:30	Yes / **No**

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

12.1.10 Xept on Holiday

Default: No
Selections:
– 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.

Further information
Holiday #, page 232

RPS Menu Location
Schedules > Open/Close Windows > Xept on Holiday

12.1.11 Holiday

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, page 231* 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 to 8

12.1.12 Area

Default: No
Selections:
– 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.

RPS Menu Location
Schedules > Open/Close Windows > Area #

12.2 User group windows

Use the parameters in this section to make User Group Windows. When you assign a user group to one of the windows, the credentials (passcode, access card or token, and RF keyfob) for each user in the user group are enabled for the time between the Enable Time and Disable Time for the window.
Each user group can be assigned to multiple user group windows within a 24-hour period. Refer to User Configuration > User Assignments > *User Group, page 152*, to assign users to a user group. If a user is not assigned to a user group or the user group is not assigned to a user group window, the credentials for that user are always enabled.

12.2.1 User Group

Default: 1
Selections:
– B6512: 0 to 6
The selection of 0 is Unassigned.
Select a user group in this parameter. The user credentials (passcode, access card or token, and RF keyfob) for the users assigned to the user group are enabled for the time between the Enable Time and Disable Time for the user group window.
You can assign a user group to more than one user group window in a 24 hour period, but the windows must not overlap or exceed the midnight boundary.
If you have created specific names for the parameter, the name will show as <*Index number*>: <*descriptive name*> in the parameter selection.

RPS Menu Location
Schedules > User Group Windows > User Group

12.2.2 Sunday through Saturday

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.

Further information
Xept Holiday, page 231

RPS Menu Location
Schedules > User Group Windows > Sunday through Saturday

12.2.3 Group Enable Time

Default: Disable
Selections: Disable, HH:MM (hours and minutes)
Beginning at the time you enter here, the credentials (passcode, access card or token, and RF keyfob) for each user in the user group are enabled. The window starts at the beginning of the minute.
In the **Time Input** pop-up window, enter the time of day that the window starts. Use the 24-hour time format (for example, enter 7:00 AM as 07:00, enter 2:45 PM as 14:45).
If you check **Disable** in the Time Input pop-up window, the Group Enable Time reverts to 00:00.
To start a window at the time you enter here on the same day you configure the control panel, select **Reset Panel** when you disconnect RPS from the control panel.

RPS Menu Location
Schedules > User Group Windows > Group Enable Time

12.2.4 Group Disable Time

Default: Disable
Selections: Disable, HH:MM (hours and minutes)
The time you enter here is the end of the user group window. The credentials (passcode, access card or token, and RF keyfob) for each user in the user group are disabled. The window ends at the end of the minute.
In the **Time Input** pop-up window, enter the time of day when the window ends. Use the 24-hour time format (for example, enter 7:00 AM as 07:00, enter 2:45 PM as 14:45).
If you check **Disable** in the Time Input pop-up window, the Group Disable Time reverts to 00:00.
To end a window at the time you enter here on the same day you configure the control panel, select **Reset Panel** when you disconnect RPS from the control panel.

RPS Menu Location
Schedules > User Group Windows > Group Disable Time

12.2.5 Xept Holiday

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

12.2.6 Holiday

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 #

12.3 Skeds

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).

12.3.1 Sked Name Text

Default: Sked #
Selections: Up to 32 alphanumeric characters
Enter up to 32 characters of text to describe the area.

RPS Menu Location
Schedules > Skeds > Sked Name Text

12.3.2 Sked Name Text (Second Language)

Default: blank
Selections: Up to 32 alphanumeric characters
Enter up to 32 characters of text to describe the area.

RPS Menu Location
Schedules > Skeds > Sked Name Text (second language)

12.3.3 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

12.3.4 Function

Default: Not in Use

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.

Notice!

The All On - No Exit feature is ignored when arming from a SKED.

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

All On Delay, page 235
All On Instant, page 236
Part On Delay, page 236
Part On Instant, page 236
Disarm, page 236
Extend Close, page 236
Bypass a Point, page 236
Unbypass a Point, page 236
Unbypass All Points, page 236
Turn Output On, page 237
Turn Output Off, page 237
Toggle Output, page 237
Reset All Outputs, page 237
Unlock Door, page 237
Lock Door, page 237
Secure Door, page 237
Access Ctrl Level, page 237
Access Granted Events, page 237
Access Denied Events, page 238
Contact RPS, page 238
Contact RPS User Port, page 238
Send Status Report, page 238
Send Test Report, page 238
Send Test on Off Normal, page 240
Watch On, page 240

Watch Off, page 240
Show Date & Time, page 240
Sound Watch Tone, page 240
Set Keypad Volume, page 241
Set Keypad Brightness, page 241
Execute Custom Function, page 241

RPS Menu Location
Schedules > Skeds > Sked 1-80 > Function

12.3.5 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 OK.

RPS Menu Location
Schedules > Skeds > Time

12.3.6 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

12.3.7 Sunday through Saturday

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 on Holiday, page 235* 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

12.3.8 Xept on Holiday

Default: No
Selections:
– 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

12.3.9 Holiday

Default: No
Selections:
– Yes - use the holiday index with this User Group Window.
– No - do not use the holiday index with this User Group Window.

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 > Skeds > Holiday #

12.4 Holiday indexes

12.4.1 Schedule

Holiday Indexes Schedule
Use this parameter to schedule holidays in a Holiday Index.
For each Holiday Index, you can schedule up to 365 (366 for leap years) as holidays.
Click the Holiday Index you wish to schedule holidays for. The holiday schedule dialog looks like a calendar. It shows the current month and year by default. The year is for reference purposes only. Only month and day data is sent to the control panel.
When you set a day on the calendar as a holiday that day is a holiday every year thereafter. For example, if you set October 26, 2019, as a holiday, October 26 is a holiday in 2020, 2021, and so on. The day of the week changes according to the year.

RPS Menu Location
Schedules > Holiday Index > Holiday Indexes Schedule

12.5 Sked Function descriptions

12.5.1 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.

12.5.2 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.

12.5.3 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.

12.5.4 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.

12.5.5 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.

12.5.6 Extend Close

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

Notice!
Extend Close time cannot extend past midnight. If enabled, it cannot extend past an area's configured Latest Close Time.

12.5.7 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 Profile assigned to the point. The bypass is reported if Bypass Reports are enabled in the Point Profile assigned to the point. The Sked can bypass one point.

12.5.8 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.

12.5.9 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.

Notice!
Faulted 24-hour points are not unbypassed
To prevent point alarm or trouble events, bypassed 24-hour points that are faulted when this Sked function runs are not unbypassed. They remain bypassed.

12.5.10 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.

12.5.11 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.

12.5.12 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.

12.5.13 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.

12.5.14 Unlock Door

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

12.5.15 Lock Door

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

12.5.16 Secure Door

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

12.5.17 Access Ctrl Level

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

12.5.18 Access Granted Events

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

12.5.19 Access Denied Events

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

12.5.20 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.

Notice!
Avoid having multiple functions occur at the same time at the same address. Functions can clash and the effect on the panel is unpredictable.

Notice!
Do not program multiple Skeds to execute at the same keypad during the same time of execution.

Notice!
Do not program Skeds to execute at times when a user is likely to be executing functions at the keypad.

12.5.21 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.

12.5.22 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.

Notice!
Sked executed reports conflict
Disable Sked Executed reports if you are using Deferred Test or Status reports. These reports will not run if Sked Executed reports are enabled.

12.5.23 Send Test Report

This sked function sends the same test report as the user Test Report function.
You can send test reports to 1 or all destinations that are configured for a Route Group. Primary and First, Second, Third Backup Destination Devices can send manual and automatic (scheduled) test reports.
If a point in any area is off normal (trouble not cleared from the keypad display), the control panel sends a test off-normal report instead of the test report.

If the Panel Wide Parameters > Report Routing > *Expand Test Report, page 33* parameter is set to Yes, the test report (or test off-normal report) is followed by a diagnostic report for each off-normal system status. Refer to Panel Wide Parameters > Report Routing > *Diagnostic Reports, page 59* for a list of reports included.

Selections, Parameter 1: Deferred

– Yes - defer sending test reports for 24 hours if the control panel sends any other report.
– No - do not defer sending test reports.

Notice!
Only sending the test report is deferred
When Parameter 1: Deferred is set to Yes, only sending the test report is deferred. The Send Test Report sked still runs at the frequency set in Parameter 2: Frequency.

Selections, Parameter 2: Frequency

– Hourly - the first Send Test Report sked runs at the time entered in the Time parameter for the Sked. The Send Test Report sked runs every hour after that.
– Monthly - the first Send Test Report sked runs at the time entered in the Time parameter for the sked, on the date entered in the Date parameter. The Send Test Report sked runs every month after that.
– Scheduled - the Send Test Report sked runs according to the sked Time, Date, and days of week parameters.

Notice!
When Parameter 2 is set to Scheduled and a date is entered in the Date parameter, the days of week parameters are ignored
The control panel sends the test report on the date and time entered in the sked Date and Time parameters.

Selections, Parameter 3

When Parameter 3 is configured for any Route Group (Primary, First, Second or Third Backup Destination Device), Parameter 4 for destinations is enabled. See *Communicator, overview, page 63* for Route Group configuration information.

Selections, Parameter 4

When Parameter 4 is enabled, all configured Route Group destinations are shown. Select the checkbox of the Route Group(s) that you want to use as a destination.

Deferring test reports

When Parameter 1: Deferred is set to Yes, the control panel starts (or restarts) a 24 hour countdown timer each time it receives an Ack (acknowledgement) from the central station receiver for any report.
If Parameter 2 is set to Hourly, and the panel has not received an Ack by the time the first hourly Send Test Report sked runs, the panel sends the test report. If the panel received an Ack, test reports are deferred for 24 hours from the last Ack received. The hourly Send Test Report sked will not send a test report for at least 24 hours.
If Parameter 2 is set to Monthly, and the panel has not received an Ack within 24 hours of the time the first monthly Send Test Report sked runs, the panel sends the test report. If the panel receives an Ack within 24 hours of the time a monthly Send Test Report sked is set to run, the test report is deferred for 24 hours from the last Ack received. If the 24 hour countdown timer expires, the panel sends the deferred test report at that time.

If Parameter 2 is set to Scheduled, and the panel has not received an Ack within 24 hours of the time the scheduled Send Test Report sked runs, the panel sends the test report. If the panel receives an Ack within 24 hours of the time a scheduled Send Test Report sked is set to run, the test report is deferred for 24 hours from the last Ack received. If the 24 hour countdown timer expires, the panel sends the deferred test report at that time.

Notice!
Sked executed reports conflict
Disable Sked Executed reports if you are using Deferred Test or Status reports. These reports will not run if Sked Executed reports are enabled.

Report Routing configuration
For the Report Routing configuration for test reports, test off-normal reports, and expanded test reports, refer to Panel Wide Parameters > Report Routing > Test Reports > *Test Reports, page 58*.

12.5.24 Send Test on Off Normal

When this sked function runs and a point in any area is off normal (trouble not cleared from the keypad display), the control panel sends a test off-normal report. If there no points off normal when this sked runs, the control panel does not sent a report.
If the Panel Wide Parameters > Report Routing > *Expand Test Report, page 33* parameter is set to Yes, a test off-normal report is followed by a diagnostic report for each off-normal system status. Refer to Panel Wide Parameters > Report Routing > *Diagnostic Reports, page 59* for a list of reports included.

12.5.25 Watch On

This function emulates the operation of the keypad shortcut Change Watch Mode by activating Watch 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.

12.5.26 Watch Off

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

12.5.27 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 #.

Notice!
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.

12.5.28 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 tone.
Stop the tone by any interaction with the keypad or silence the tone by pressing [ESC].

12.5.29 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, page 121* in the keypad configuration section for details on volume parameters.

12.5.30 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, page 121* parameter in the keypad configuration section for details on the brightness parameter.

12.5.31 Execute Custom Function

This function executes the custom function selected in Parameter 1: Custom Function # at a scheduled time.

13 Access

13.1 Door

Use the parameters in this section to configure each door.

13.1.1 Door Name Text

Default: Door ##
Selections: Up to 32 alphanumeric characters
The B6512 supports Doors 1 to 4.
Enter up to 32 characters of text to describe the door.

RPS Menu Location
Access > Doors > Door Name Text

13.1.2 Door Name Text (second language)

Default: blank
Selections: Up to 32 alphanumeric characters
The B6512 supports Doors 1 to 4.

Enter up to 32 characters of text to describe the door.

RPS Menu Location
Access > Doors > Door Name Text (second language)

13.1.3 Entry Area

Default: 1
Selections:
– B6512: 1-6
Assign an area to the door controller. This is the area a user exit when initiating a request to exit (REX).

RPS Menu Location
Access > Doors > Entry

13.1.4 Associated Keypad

Default: No Keypad
Selections: 0 to 32
– B6512: 1 to 12
This parameter sets the door controller to SDI2 keypad associated for KP# Dual Authentication. A Setting of Disabled also disables Dual Authentication operation.
Enter the Keypad number (KP#) which determines the scope of the user ID's disarming rights. Areas disarm on the basis of this Keypad's scope and the Authority Level of.
No Keypad: Only the area assigned to the Entry Area disarms for this door.

RPS Menu Location
Access > Doors > Associated Keypad #

13.1.5 Custom Function

Default: Disabled
Selections:
– B6512G: Disabled, CF128 to CF133
Disabled: Custom function is disabled.

CF###: The custom function number that activates when a valid ID is entered, given the appropriate user access level and area arm state.
Use this parameter to program a custom function that activates at the keypad programmed for Scope.
This custom function only activates for users with a function level authority that allows a valid ID to perform a custom function during the armed or disarmed state.
The user to which the card or token is assigned must have an assigned passcode.
The following table shows how this programming affects custom function activation:

Function level	Custom function activation
A (armed)	User token activates the custom function assigned to the door controller only when the entry area for the door controller is All On or Part On.
D (disarmed)	User token activates the custom function assigned to the door controller only when the entry area for the door controller is disarmed.
C (armed and disarmed)	User token activates the custom function assigned to the door controller regardless of the armed state of the entry area.
Blank	User token does not activate the custom function assigned to the door controller.

RPS Menu Location
Access > Doors > Custom Function #

13.1.6 Door Point

Default: 0
Selections: 0 (no point assigned), 1-96
Use this parameter to assign a point to a door. This point cannot be used for any other point assignments.
Door Points must be programmed as Part On points. If a Door Point requires 24 hour point type behavior, use the Part On point type with a Point Response of 9 to C for instant alarm response when the area is on (armed) or off (disarmed).
If you select an on-board point (points 1-8) as a Door Point, be sure there is no EOL resistor connected to the sensor loop on the control panel.
Do not enable any POPIT points (or OctoPOPIT points) with the same point number as the Door Point. Using the same point number for the Door Point and a POPIT or OctoPOPIT point creates an Extra Point trouble.

RPS Menu Location
Access > Doors > Door Point

13.1.7 Door Point Debounce

Default: 600 ms

Selections:

Debounce		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

This parameter sets the length of time the access control module scans a door point before initiating an alarm. For appropriate settings, consult the manufacturer's instructions for the device connected to the door point.

RPS Menu Location
Access > Doors > Door Point Debounce

13.1.8 Interlock Point

Default: 0
Selections: 0 (no point assigned), 1-96
Use this parameter to make a point an Interlock Point. An Interlock Point cannot be used for any other point assignments.
Interlock Points must be programmed as Part On points. If an Interlock Point requires 24 hour point type behavior, use the Part On point type with a Point Response of 9 to C for instant alarm response when the area is on (armed) or off (disarmed).
When an Interlock Point is, faulted, it prevents the access control module from granting access for a valid ID read or door request.
You may use the same point as the Interlock Point for multiple access control modules. Sharing a point as the Interlock point for multiple modules allows one faulted point to prevent multiple modules from granting access.
The interlock point will be considered in a normal state if it is bypassed, swinger bypassed, or forced armed. This results in normal operation of access even if the door is left open.

RPS Menu Location
Access > Doors > Interlock Point

13.1.9 Auto Door

Default: No
Selections:
- Yes - when the area assigned in the Entry Area parameter is Off (disarmed), the door state is automatically Unlocked.
- No - when the area assigned in the Entry Area parameter is Off (disarmed), the door state is not changed. The previous state of the door remains the same (locked or unlocked).

Use this parameter to unlock the door (latched shunt and strike) automatically when the Entry Area parameter is Off (disarmed). The door re-locks when the area is set to All On or Part On (armed).
This parameter does not affect the armed state of the area. When the area assigned to the door Entry Area parameter is armed All On or Part On, the door state will automatically change to locked regardless of the Auto Door parameter setting (Yes or No).

Notice!
Use Secure Door to override unlocked
You cannot manually override the unlocked state. Use Secure Door to override this setting.

RPS Menu Location
Access > Doors > Auto Door

13.1.10 Fire Unlock

Default: No
Selections:
Yes: Fire or Gas alarm in any area unlocks the door.
No: Door remains in its current mode upon a Fire or Gas alarm.
Use this parameter to unlock the door strike output and shunt the door point when a Fire or Gas alarm occurs. A Door Unlock event will process. This feature overrides a Secure Door state, a Locked Door state, and an Interlock faulted point. Once a Fire Unlock occurs, you must manually re-lock the door from a keypad.

Notice!
This unlocks the door regardless of the armed state.

Notice!
You can return doors activated by Fire Unlock to a normal state by pressing 8 - Main menu > 3 - Actions > 8 - Access, or through the keypad with Command 46 - Access menu.

Notice!
For door controllers configured for dual authentication, Fire Unlock is only available if you configure the associated keypad with a Passcode Enter Function of Cycle Door. All other Passcode Enter functions use the token reader for authentication and prevent all door functions including Fire Unlock.

RPS Menu Location
Access > Doors > Fire Unlock

13.1.11 Disarm on Open

Default: No
Selections:
Yes: the area only disarms after access has been granted to a user with disarm authority, and the door point has been faulted (door was opened).
No: the area disarms when a user with a valid disarm level presents a valid token/card, whether or not the door has been opened.
Use this program item to determine whether the door needs to be physically opened prior to disarming the area upon a valid access request. The user initiating the access request must have access levels that allow disarming with ID.

RPS Menu Location
Access > Doors > Disarm on Open

13.1.12 Strike Time

Default: 10

Selections: 1 - 240 seconds

The strike activates for the amount of time programmed.

Enter the amount of time the output for the strike activates to allow a user to open the door. The strike activates upon a valid credential (card), Request to Enter (RTE), Request to Exit (REX), and the keypad [CYCLE DOOR?] function.

RPS Menu Location

Access > Doors > Strike Time

13.1.13 Shunt Time

Default: 10

Selections: 0 - 254

You can set the door Shunt Time in seconds, minutes or hours.

Enter the length of time the door is shunted to allow a user to open the door without causing the point to go into Trouble, Alarm, or faulted condition.

Notice!

For SDI connected doors, the panel will automatically apply the maximum of 240.

For SDI2 connected doors, a panel without firmware supporting the larger Shunt Times will apply entries above 240 as seconds.

Selection	Time Value
0-240	0-240 seconds
241	5 minutes
242	10 minutes
243	20 minutes
244	30 minutes
245	40 minutes
246	50 minutes
247	60 minutes
248	2 hours
249	3 hours
250	4 hours
251	5 hours
252	6 hours
253	7 hours
254	8 hours

RPS Menu Location

Access > Doors > Shunt Time

13.1.14 Buzz Time

Default: 2

Selections: 0, 1 - 240 seconds

0: no buzz time for this door.

1 - 240: The buzzer sounds for seconds programmed.

Enter the seconds that the buzzer output activates to notify the user that the strike is activated and the door is ready to open. The buzzer stops when the door is opened.

A separate buzzer is required.

Many readers have an internal buzzer that is not affected by Buzz Time.

RPS Menu Location

Access > Doors > Buzz Time

13.1.15 Extend Time

Default: 10

Selections: 0, 1 - 30 seconds

Enter the amount of time (1 to 30) to prolong strike, buzz, and shunt activation when the shunt time expires and a door remains open. At the end of the programmed Extend Time, the buzzer continues to buzz until the door closes. In addition, if programmed, the point assigned to the door indicates a Trouble, Alarm, or Fault at the keypad.

Regardless of the door point programming, the system generates a Trouble Door Left Open event while the system is disarmed, and an Alarm Door Left Open event when the system is armed and the door is held open beyond Extend Time. "Door Closed - Restoral" events are generated after the door is held open past Extend Time and the door has returned to normal.

Enter 0 to disable Extend Time. The Trouble Door Left Open event, the Alarm Door Left Open event, and the warning at the keypad are all disabled.

RPS Menu Location

Access > Doors > Extend Time

13.1.16 Deactivate on Open

Default: Yes

Selections:

Yes: Strike deactivates when the door point is faulted (door is opened) after access is granted.

No: Strike remains activated for the amount of the programmed strike time or strike deactivates when the door point is faulted (door is opened) and restored (closed) after access is granted, whichever happens first.

This parameter determines whether the strike deactivates immediately upon physically opening the door (door point is faulted).

In order for this function to work, a point needs to be assigned in the Door Point parameter.

To reduce false alarms when the door "bounces" open, leave this parameter at Yes (default).

RPS Menu Location

Access > Doors > Deactivate On Open

13.1.17 RTE Shunt Only

Default: No

Selections:

Yes - when the RTE Input (Request To Enter) on the access control module is shorted the door point is shunted for the duration of Shunt Time. The strike output is not activated.

No - when the RTE Input on the access control module is shorted the door point is shunted for the duration of Shunt Time. The strike output is activated for the duration of Strike Time. Use this parameter when a user can open a door manually without relying on a token/card to activate the strike (such as with a "push bar").

Notice!
No RTE Events when RTE Shunt Only is set to Yes
When RTE Shunt Only is set to Yes, the control panel does not log or report Request To Enter events when the RTE Input is shorted.

RPS Menu Location
Access > Doors > RTE Shunt Only

13.1.18 RTE Input Debounce

Default: 600 ms
Selections:

Debounce		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

This parameter sets the length of time the access control module scans the RTE input before initiating a request to enter (RTE) event. For appropriate settings, consult the manufacturer's instructions for the device connected to the RTE input.

RPS Menu Location
Access > Doors > RTE Input Debounce

13.1.19 REX Shunt Only

Default: No
Selections:
Yes - Programmed shunt time will activate so door can be manually opened.
No - Request to Exit (REX) automatically activates the programmed strike and shunt time. Use this program item to disable the strike, but still activate the programmed shunt time upon a Request to Exit an area.
Use this parameter when a user can open a door manually without relying on a token/card to activate the strike (such as with a "push bar").
When this REX Shunt Only parameter is set to Yes, Request to Exit events are not logged or reported.

RPS Menu Location
Access > Doors > REX Shunt Only

13.1.20 REX Input Debounce

Default: 600 ms
Selections:

Debounce		
300 ms	1800 ms	3300 ms
600 ms	2100 ms	3600 ms
900 ms	2400 ms	3900 ms
1200 ms	2700 ms	4200 ms
1500 ms	3000 ms	4500 ms

This parameter sets the length of time the access control module scans the REX input before initiating a request to exit (REX) event. For appropriate settings, consult the manufacturer's instructions for the device connected to the REX input.

RPS Menu Location
Access > Doors > REX Input Debounce

13.1.21 Access Granted

Default: Yes
Selections:
Yes: ACCESS GRANTED and DOOR REQUEST events logged and reported.
No: ACCESS GRANTED and DOOR REQUEST events are not logged or reported.
This parameter determines if ACCESS GRANTED and DOOR REQUEST events from this access control module are logged and reported by the control panel.
An ACCESS GRANTED event can be initiated by:
– a valid read of a crendential (card or token)
– a valid door state changed at the keypad

RPS Menu Location
Access > Doors > Access Granted

13.1.22 No Entry

Default: Yes
Selections:
Yes: ACCESS DENIED events logged and reported.
No: ACCESS DENIED events are not logged and reported.
This No Entry parameter determines if ACCESS DENIED events from this access control module are logged and reported by the control panel.
A No Entry (ACCESS DENIED) event may be caused by:
– invalid or unknown user ID, interlock or secured door, or incorrect authority level
– request to enter/exit (RTE/REX) for door in interlock or secured door

RPS Menu Location
Access > Doors > No Entry

13.1.23 Enter Request

Default: No
Selections:
Yes: Request to Enter (RTE) events are logged and reported.
No: Request to Enter (RTE) events are not logged and reported.
This parameter determines if Request to Enter (RTE) events from this access control module are logged and reported by the control panel.

Modem 4 format is supported. Contact ID is not supported. If Yes is selected, RTE or REX events with contact ID is not reported.

RPS Menu Location
Access > Doors > Enter Request

13.1.24 Exit Request

Default: No
Selections:
Yes: Request to Exit (REX) events are logged and reported.
No: Request to Exit (REX) events are not logged and reported.
This parameter determines if Request to Exit (REX) events from the access control module are logged and reported by the control panel.
Modem 4 format is supported. Contact ID is not supported. If Yes is selected, RTE or REX events with contact ID is not reported.

RPS Menu Location
Access > Doors > Enter Request

13.1.25 Failure Mode

Default: Fail secure
Selections:
Fail Secure. Door remains locked to ensure continued security.
Fail Safe. Access module releases door locking mechanism to allow passage.
This parameter sets the behavior for the Access Module when it loses communication with the control panel and enters Failure Mode.
This configuration option only applies to the SDI2 B901 access control modules.

RPS Menu Location
Access > Doors > Failure Mode

13.1.26 Enclosure Tamper

Default: No
Selections:
Yes - enable tamper input (T+).
No - disable tamper input (T+).

Notice!
Enclosure Tamper parameter configures reader tamper input, T+
For the B901 Access Control Interface module, this parameter enables the reader tamper input (T+ terminal). There is no enclosure tamper input on these modules.

For a D9210C or B901 on the SDI bus (Door Source = SDI) shorting the tamper input (T+) to common (COM) creates a Point Missing event for the *Door Point, page 243*.
For a B901 on the SDI2 bus (Door Source = SDI2 (B901)) shorting the tamper input (T+) to common (COM) creates a Point Missing event for the *Door Point, page 243* and a Tamper event for the B901 module.

RPS Menu Location
Access > Doors > Enclosure Tamper

13.2 Global Access settings

13.2.1 Card Type

Default: 26 bit

Selections:

– 26 bit
– 32 bit MIFARE Classic
– 35 bit Corporate 1000
– 37 bit no site code
– 37 bit with site code

This parameter specifies the card or token format used for all of the door controllers and keypads.

Set to 26 bit when credentials (card or token) are used with a B942 keypad.

Default Site Codes for card types

26 bit: default site code is 255.

32 bit: default site code is blank. The site code is not configurable (Site Code parameter is grayed out).

35 bit: default site code is 4095. Enter the site code (facility code) during configuration of a user access card.

37 bit no site code: default site code is blank. The site code is not configurable (Site Code parameter is grayed out).

37 bit with site code: default site code is 65535.

RPS Menu Location

Access > Global Keypad Settings > Card Type

13.3 Door Source

Default: Disabled

Selections:

– Disabled. Door module is disabled.
– SDI2 (B901)

Use this parameter to assign each door to a device type.

RPS Menu Location

Access > Doors > Door Source

14 Automation / Remote App

14.1 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 B426 module at SDI2 address 2.
- Mode 1 using onboard connection with TLS.
- Mode 2 (using an onboard connection or B426 module at SDI2 address 1-2 with TLS).

RPS Menu Location

Automation / Remote App > Automation Device

14.2 Status Rate

Default: 0

Selections:

- 0 - status information never sent unless requested.
- 1 - 255 - status information is sent at the interval programmed.

This parameter sets how often the default status information is sent to the Serial Interface Module.

The Status information includes the current point status (normal or off-normal), the control panel's area status (All On, All On Instant, Part On Delay Armed, Part On Instant, 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 500 millisecond increments. Therefore, if a 5 is entered, the Status information is sent every 2500 milliseconds (or 2.5 seconds). An entry of 10 would equal 5 seconds. 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 1.5 to 2 seconds.

RPS Menu Tree Location

Automation / Remote App > Status Rate

14.3 Automation Passcode

Default: Blank

Selections: 6 to 24 characters.

This parameter sets the passcode that must be entered before automation software can connect to the control panel.

This parameter accepts up to 24 characters, but allows shorter passcodes. The minimum length is six characters. The passcode is case-sensitive. The automation passcode must be entered before any other automation commands will be accepted by the control panel.

Notice!
UL 2610 requirement
For UL 2610 compliance, the password length must be at least 6 characters and contain a combination of numbers, letters and symbols.

RPS Menu Tree Location
Automation / Remote App > Automation Passcode

14.4 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 Location
Automation / Remote App > Mode 1 Automation Ethernet Port Number

14.5 Remote App

Default: Enable
Selections:
- Enable - the control panel is able to establish secure connections with remote apps.
- Disable - the control panel is not able to establish secure connections with remote apps.

Set this parameter to Enable, to allow the control panel to establish secure connections with remote apps. The Bosch Remote Security Control app for smart phones and tablets is an example of a remote app.
Set this parameter to Disable, to prohibit the control panel from establishing secure connections with remote apps.

RPS Menu Location
Automation / Remote App > Remote App

14.6 Remote App Passcode

Default: [RPS generated random 24 character passcode]
Selections: 6 to 24 case sensitive, alphanumeric characters:
A-Z, a-z, 0-9,!@#$%^&"()-_+=|` ~,<.>/?;:'"[\{]}

Use this parameter to set the control panel passcode for remote applications to establish a secure control panel connection. For example, Bosch Remote Security Control (RSC) and Bosch Security Manager (BSM) mobile apps. The passcode is exchanged and validated by the control panel before any other commands or control panel user passcodes are accepted by the control panel.

Notice!
UL 2610 requirement
For UL 2610 compliance, the password length must be at least 6 characters and contain a combination of numbers, letters and symbols.

When updating a control panel Remote App Passcode, all current users of remote applications, such as RSC or BSM, lose the ability to connect until their app also receives a new connection profile that includes the new Remote App Passcode.

To update users of:

– Bosch Security Manager app - an update to Installer Services will update the control panel connection profile for all current mobile app users. RPS updates Installer Services during specific activities if it is able to reach online services.
  RPS attempts to auto-update Installer Services with control panel details during a new user invite to the Bosch Security Manager app and during a control panel connection/ programming synchronization.
  RPS operators can update Installer Services with panel details at any time by navigating to Manage Bosch Security Manager App Users and selecting Update Installer Services Mobile Profile.
– Remote Security Control app - use the RPS Build Remote Access Profile to create a new connection profile for the control panel and distribute to each individual mobile app.
– SDK Intrusion Integrations - use the RPS Build Remote Access Profile to create a new connection profile for the control panel and distribute to each integrator.

Notice!

Disable Remote App Passcode to disable remote app login

To prevent any remote app (RSC or BSM) user from logging into the control panel, even when the Remote App parameter is set to Enable, set the Remote App Passcode to Disabled (any combination of upper and lower case characters).

RPS Menu Location

Automation / Remote App > Remote App Passcode

15 SDI2 modules

15.1 B208 Octo-input

The B208 Octo-input module provides inputs (sensor loops) for 8 points. The B208 connects to the SDI2 bus of the control panel.

Panel type	Modules supported
B6512	8

Table 15.2: Capacity

Switch Settings
Refer to Hardware Switch Settings > *B208 Octo-input Module switch settings, page 270*

15.1.1 Enclosure Tamper

Default: No - Disable
Selections:
– Yes - enable enclosure tamper input
– No - disable enclosure tamper input
When the tamper input is enabled and connected to a Bosch ICP-EZTS tamper switch, the control panel creates a tamper event when the enclosure door is opened, or when the enclosure is removed from the wall.

RPS Menu Location
SDI2 modules > B208 Octo-input > Enclosure Tamper

15.2 B308 Octo-output

The B308 Octo-output is a device that attaches to the SDI2 bus of the control panel. Each module provides 8 independently monitored outputs similar in function to those provided by the output modules.

Panel type	Modules supported
B6512	8

Table 15.3: Capacity

Switch Settings
Refer to Hardware Switch Settings > *B308 Octo-output Module switch settings, page 270*

15.2.1 Enclosure Tamper

Default: No - Disable
Selections:
– Yes - enable enclosure tamper input
– No - disable enclosure tamper input

When the tamper input is enabled and connected to a Bosch ICP-EZTS tamper switch, the control panel creates a tamper event when the enclosure door is opened, or when the enclosure is removed from the wall.

RPS Menu Location
SDI2 modules > B308 Octo-output > Enclosure Tamper

15.3 (B42x) IP Communicator

Connecting the B42x
Connect the module to the control panel using the SDI2 bus.

Configuring the module
You can use one or both B426/B450 communication modules for central station reporting or RPS communications. Or, you can use one of the B42x modules for communication with automation software.

Notice!
To prevent communication loss, the configuration sent to the control panel for the B42x module takes effect after RPS disconnects from the control panel.
If the module is configured through the B42x configuration web interface to disable control panel programming (that is, Panel Programming Enable is set to No), then RPS programming of the B42x is accepted by the control panel, but not applied to the B42x. The Panel Programming Enable parameter is not available in RPS.

15.3.1 Module Enclosure Tamper

Default: No - Disable
Selections:
– Yes - enable enclosure tamper input
– No - disable enclosure tamper input

When the tamper input is enabled and connected to a Bosch ICP-EZTS tamper switch, the control panel creates a tamper event when the enclosure door is opened, or when the enclosure is removed from the wall.

RPS Menu Location
SDI2 > B42x IP Communicator > Enclosure Tamper

15.3.2 IPv6 Mode

Default: No
Selections:
– Yes - use IPv6 mode (Internet Protocol version 6) for IP communications
– No - use IPv4 mode (Internet Protocol version 4) for IP communications

When IPv6 Enable is set to Yes, set DHCP/AutoIP enable to Yes.

RPS Menu Location
SDI2 > B42x IP Communicator > IPv6 Mode

15.3.3 IPv6 DHCP

Default: Enabled (Yes)
Selections:
– Enabled (Yes) - DHCP automatically sets the IP Address, IP Default Gateway, and IP DNS Server Address. AutoIP enables dynamic IP addresses to be assigned to devices at start-up.

– Disabled (No) - Set this parameter to Disabled if there is no DHCP service. Manually set the IP Address, IP Default Gateway, and IP DNS Server Address.

DHCP requires a DHCP server.

RPS Menu Locations

SDI2 > B42x IP Communicator > IPv6 DHCP

15.3.4 IPv4 DHCP/AutoIP Enable

Default: Enabled (Yes)

Selections:

– Enabled (Yes) - DHCP automatically sets the IP Address, IP Default Gateway, and IP DNS Server Address. AutoIP enables dynamic IP addresses to be assigned to devices at start-up.

– Disabled (No) - Set this parameter to Disabled if there is no DHCP service. Manually set the IP Address, IP Default Gateway, and IP DNS Server Address.

DHCP requires a DHCP server.

The parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location

SDI2 > B42x IP Communicator > IPv4 DHCP/AutoIP Enable

15.3.5 IPv4 Address

Default: 0.0.0.0

Selections: 0.0.0.0 to 255.255.255.255

If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).

If IPv4 DHCP/Auto IP Enable is set to No, enter the IPv4 address here.

This parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location

SDI2 > B42x IP Communicator > IPv4 address

15.3.6 IPv4 Subnet Mask

Default: 255.255.255.0

Selections: 0.0.0.0 to 255.255.255.255

If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).

If IPv4 DHCP/Auto IP Enable is set to No, enter the IPv4 sub-network mask here.

The parameter has no effect on B450 Plug-in Communicator Interface operation.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location

SDI2 > B42x IP Communicator > IPv4 Subnet Mask

15.3.7 IPv4 Default Gateway

Default: 0.0.0.0

Selections: 0.0.0.0 to 255.255.255.255

If IPv4 DHCP/Auto IP Enable is set to Yes, this parameter is grayed out (no access to it).

If IPv4 DHCP/Auto IP Enable is set to No, enter the Default Gateway address here.

The parameter has no effect on B450 Plug-in Communicator Interface operation.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location
SDI2 > B42x IP Communicator > IPv4 default gateway

15.3.8 IPv4 DNS Server IP Address

Default: 0.0.0.0
Selections: 0.0.0.0 to 255.255.255.255
A Domain Name Server (DNS) uses internet domain names or hostnames to supply corresponding IP addresses. In DHCP mode, the DHCP server's default DNS is used. To use a custom DNS server in DHCP mode, enter the custom DNS server's IP address here.

RPS Menu Location
SDI2 > B42x IP Communicator > IPv4 DNS server IP address

15.3.9 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 sets the IPv6 DNS server address for Static IP mode.
When this address is set by the DHCP service, do not change it.

Further information
IP Address and Domain Name formats, page 275

RPS Menu Location
SDI2 > B42x IP Communicator > IPv6 DNS server IP address

15.3.10 UPnP (Universal Plug and Play) Enable

Default: Yes
Selections:
Yes (Enabled) – use UPnP to open a port forwarder for inbound RPS and RSC (Remote Security Control) connections
No (Disabled) – do not use UPnP
The UPnP parameter has no effect on event reporting to a central station receiver.
The UPnP parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location
SDI2 > B42x IP Communicator > UPnP enable

15.3.11 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.

RPS Menu Location
SDI2 Modules > IP Communicator > HTTP Port Number

15.3.12 ARP Cache Timeout (sec.)

Default: 600
Selections: 1 to 600 (seconds)
This parameter specifies the time-out for ARP cache entries.

The parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location
SDI2 > B42x IP Communicator > ARP cache timeout

15.3.13 Web/USB Access Enable

Default: No
Selections: Yes/No
This parameter enables authorized users to view and modify the module configuration parameters through a standard web browser or USB, depending on available options.

RPS Menu Location
SDI2 Modules > IP Communicator > Web/USB access Enable.

15.3.14 Web/USB Access Password

Default: Blank
Selections: blank, ASCII printable characters
This parameter sets a new password required for direct logins using web access. The password must be 4-10 ASCII printable characters in length. Blank spaces disable the password checking.

Notice!
UL 2610 requirement
For UL 2610 compliance, the password length must be at least 6 characters and contain a combination of numbers, letters and symbols.

Notice!
The default passcode for the B426 module is located on a label affixed to the module.

RPS Menu Location
SDI2 > IP Communicator > Web Access Password

15.3.15 Firmware Upgrade Enable

Default: No
Selections:
Yes - modify the firmware through the web interface.
No - modify the firmware through the programming software.
This parameter allows the module firmware to be modified using the external Web interface.

RPS Menu Location
SDI2 Modules > IP Communicator > Firmware Upgrade Enable

15.3.16 Module Hostname

Default: Blank
Selections: 1-63 characters, a-z, A-Z, 0-9, hyphen (-) in the 0000.0000.0000.0000 format. Note that the module hostname cannot begin or end with a hyphen (-).
The hostname identifies the IP communicator (onboard or SDI2 module) on the network. Leave this parameter blank to use the factory default hostname.
The parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location
SDI2 > B42x IP Communicator > Module Hostname

15.3.17 Unit Description

Default: Blank
Selections: Up to twenty alphanumeric characters.
This parameter describes the module (location, attributes, etc.) in up to 20 characters. Use only the following characters: A to Z, 0 to 9, ?, &, @, -, *, +, $, #, /

RPS Menu Location
SDI2 Modules > IP Communicator > Unit Description.

15.3.18 TCP/UDP Port Number

Default: 7700
Selections: 0 - 65535
For IP communications with RPS, automation, or Remote Security Control (RSC) in typical installations, keep the TCP/UDP Port at the default

RPS Menu Location
SDI2 Modules > IP Communicator > TCP/UDP Port Number

15.3.19 TCP Keep Alive Time

Default: 4 minutes
Selections: Off - 8 Hours
Time between TCP keep-alive messages can be set in either minutes or hours. Keep alive messages make sure that a connection stays active.
The parameter has no effect on B450 Plug-in Communicator Interface operation.

RPS Menu Location
SDI2 > B42x IP Communicator > TCP keep alive time

15.3.20 IPv4 Test Address

Default: 8.8.8.8
Selections: IPv4 address or Domain Name
The control panel pings the IPv4 Test Address to make sure the network configuration settings are correct and that the network is operating.
The default test address works for most networks.

RPS Menu Location
SDI2 > B42x IP Communicator > IPv4 Test Address

15.3.21 IPv6 Test Address

Default: 2001:4860:4860::8888
Selections: IPv6 address or Domain Name
The control panel pings the IPv6 Test Address to make sure the network configuration settings are correct and that the network is operating.
The default test address works for most networks.

Further information
IP Address and Domain Name formats, page 275

RPS Menu Location
SDI2 > B42x IP Communicator > IPv6 test address

15.3.22 Web and Automation Security

Default: Enable

Selections:

– Disable - enhanced security is not applied.

– Enable - enhanced security is applied.

Set this parameter to Enable for enhanced security for Automation and B42x Web Access. When enabled, HTTPS is applied to B42x 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

15.3.23 Alternate IPv4 DNS server IP address

Default: 0.0.0.0

Selections: 0.0.0.0 to 255.255.255.255

If the IP communicator fails to get an address from the primary server, it tries the alternate DNS server. Enter the IP address for the alternate IPv4 DNS server.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location

SDI2 > B42x IP Communicator > Alternate IPv4 DNS server IP address

15.3.24 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

If the IP communicator fails to get an address from the primary server, it tries the alternate DNS server. Enter the IP address for the alternate IPv6 DNS server.

Further information

IP Address and Domain Name formats, page 275

RPS Menu Location

SDI2 > B42x IP Communicator > Alternate IPv6 DNS server IP address

15.4 B450 cellular

15.4.1 Inbound SMS

Notice!

Important configuration information for cellular communication

Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Yes

Selections:

– Enabled (Yes) - you can use inbound SMS text messages to configure the module.

– Disabled (No) - the module does not process inbound SMS text messages.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Inbound SMS

15.4.2 Session Keep Alive Period (min.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0
Selections: 0 (disabled) to 1000 (minutes)
Time in minutes between keep-alive messages. Keep alive messages make sure that a connection stays active.
Only change from default for high security UL1610 commercial listed installations.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Session keep alive period

15.4.3 Inactivity Time Out (min.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0
Selections: 0 (disable) to 1000 (minutes)
– 0 (disabled) - panel does not monitor for data traffic.
– 1 to 1000 - the time with no data traffic before the control panel ends a session.
Only change from default for high security UL 1610 commercial listed installations requiring low signal notification.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Inbound SMS

15.4.4 Reporting Delay for Low Signal Strength (sec.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0 (disabled)
Selections: 0 (disabled), 1 - 3600 (seconds)
Time of low signal strength (red LED on cellular communicator) before the control panel makes a Cellular Low Signal event.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Reporting delay for low signal strength

15.4.5 Reporting Delay for Single Tower (sec.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0
Selections: 0 (disabled) - 3600 (seconds)
Keep this parameter at the default setting unless instructed by Bosch support.
When the cellular plug-in module senses only one tower for the seconds set at this parameter, the control panel records a Single Tower event.
When the cellular communicator senses two or more towers for the seconds set at this parameter, the control panel records a Single Tower restoral event.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Reporting delay for single tower

15.4.6 Reporting Delay for No Towers (sec.)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: 0
Selections: 0 (disabled) - 3600 (seconds)
When the cellular plug-in module senses no towers for the seconds set by this parameter, the control panel records a No Towers event and a No IP Address event.
The control panel records a No Tower restoral event when the cellular plug-in module senses one or more towers for the seconds set by this parameter.
The control panel records a No IP Address restoral event when the cellular plug-in module registers with one or more towers and receives an IP address within 60 seconds.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Reporting delay for no towers

15.4.7 Outgoing SMS Length

Default: 160
Selections: 0 (disabled) to 3600 (characters)
Cellular providers set the limit for SMS message length to 160 characters (the default). The providers reject SMS messages above the limit.

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Outgoing SMS Length

15.4.8 SIM PIN

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Blank
Selections: 0-9 (minimum 4 digits, maximum 8 digits)
Use this parameter only when a PIN is necessary for ICCID cards.
If a SIM PIN is not necessary, leave the field blank.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > SIM PIN

15.4.9 Network Access Point Name (APN)

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: eaaa.bssd.vzwentp
Selections: 0-9, A-Z, a-z, **-** , **:** , **.** (up to 60 characters)
To change the access point name (APN) from the default, enter up to 60 characters. The field is case sensitive.

Control panel firmware version 3.07 or later
With control panel firmware version 3.07 or later, when the APN parameter is blank the control panel uses an internal list of Network Access Point Name (APN) values.
When a B442, B443 or B444 plug-in cellular communicator is plugged in, the internal list includes:
– Iotst.aer.net
– gne
– wyless.apn (valid only for versions earlier than RPS 6.07)
– wyless.com.attz
– bosch.vzwentp
When a B444-V plug-in cellular communicator is plugged in, the internal list includes:
– bssd.vzwentp
When a B444-A plug-in cellular communicator is plugged in, the internal list includes:
– bssd.attentp

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Network access point name (APN)

15.4.10 Network Access Point User Name

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Blank
Selections: ASCII characters (up to 30)
Enter up to 30 ASCII characters for the Network Access Point user name.
The user name is case sensitive.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Network access point user name

15.4.11 Network Access Point Password

Notice!
Important configuration information for cellular communication
Refer to *Configuring for Cellular Service, page 272* for an overview and configuration information.

Default: Blank
Selections: ASCII characters (up to 30 characters)
Enter up to 30 ASCII characters for the Network Access Point password.
The password is case sensitive.

RPS menu location
SDI2 modules > IP Communicator > B450 Cellular > Network access point password

15.5 B5xx Aux Power Supply

The B5xx Aux Power Supply connects to the SDI2 bus of the control panel. It provides a supervised 12 Volt DC 2.5 Amp auxiliary power supply.

Panel type	Modules supported
B6512, B5512	4
B4512	2
B3512	2

Switch Settings
Refer to Hardware Switch Settings > SDI2 Devices > *B5xx Aux Power Supply switch settings, page 271*

15.5.1 Module Enable

Default: No
Selections:
– Yes - supervise the SDI2 module.
– No - do not supervise the SDI2 module.

RPS Menu Location
SD12 > B520 Power Supply > Module Enable

15.5.2 Module Enclosure Tamper

Default: No - Disable
Selections:
– Yes - enable enclosure tamper input
– No - disable enclosure tamper input

When the tamper input is enabled and connected to a Bosch ICP-EZTS tamper switch, the control panel creates a tamper event when the enclosure door is opened, or when the enclosure is removed from the wall.

RPS Menu Location
SDI2 > B520 Aux Power Supply > Enclosure Tamper

15.5.3 One or Two Batteries

Default: One
Selections:
– One - one battery is connected to the B5xx BATT 1 terminals.
– Two - Two batteries are connected to the B5xx. One battery to the BATT 1 terminals and one battery to the BATT 2 terminals.

RPS Menu Location
SDI2 Modules > B5xx Aux Power Supply > One or Two Batteries

15.6 Wireless Receiver

The control panel supports two types of SDI2 wireless interface modules.
– B810 RADION receiver SD
– B820 Inovonics SDI2 bus interface
You can use only one wireless module at a time.

Notice!
Choose the type of wireless module **before** you add any points, users or repeaters to the system. When you change wireless types, RPS resets all RF information to factory defaults. All previously configured RF information is erased.

Switch Settings
Refer to B810/B820 *Hardware switch settings, page 269*

15.6.1 Wireless Module Type

Default: B810 RADION Wireless
Selections:
– Unassigned
– B810 RADION Wireless
– B820 Inovonics Wireless
This parameter configures the system for either a RADION or an Inovonics wireless module. **Unassigned**. You cannot use a wireless device. Wireless is not a valid selection for the Point Source parameter for any point. You cannot enroll RF Keyfobs for any user.

B820 Inovonics wireless capacity
Devices - 350 (not including repeaters)
Repeaters - 4
You can assign Inovonics wireless devices to points.
You can assign Inovonics keyfobs to users.

B810 RADION wireless capaciaty
Keyfobs - 1000
Points - 504 (valid point numbers: 9 to 96)
Repeaters - 8
When these limits are reached, RPS shows a warning message. To add another device of that type, delete one or more of the existing devices.

RPS Menu Location
SDI2 Modules > Wireless Receiver > Wireless Module Type

15.6.2 Module Enclosure Tamper

Default: No - Disable
Selections:
– Yes - enable enclosure tamper input
– No - disable enclosure tamper input
When the tamper input is enabled, the control panel creates a tamper event when the enclosure is opened, or when the enclosure is removed from the wall.

RPS Menu Location
SDI2 > Wireless Receiver > Enclosure Tamper

15.6.3 System (Repeater) Supervision Time

Default: 12 hours
Selections:
– None - Disable wireless repeater supervision.
– 4, 12, 24, 48, 72 hours
This parameter sets the supervision time for all configured wireless repeaters. If the wireless receiver does not hear from a repeater within the number of hours set by this parameter, the control panel creates a missing repeater event.

Notice!
Wireless Point Supervision Time
Configure the wireless supervision time for non-fire points using the parameter Point Profiles / *Wireless Point Supervision Time, page 215*. The wireless point supervision time for fire points is fixed at 4 hours.

Notice!
Wireless Keyfob Supervision Time
Enable or disable wireless supervision time for wireless keyfobs using the parameter User Assignments / *Supervised, page 154*. When supervision is enabled, the wireless keyfob supervision time is fixed at 4 hours.

RPS Menu Location
SDI2 > Wireless Receiver > System Supervision Time

15.6.4 Low Battery Resound

Default: Never Resound
Selections: Never Resound, 4 hours, 24 hours
This parameter is global for all non-fire points. The control panel automatically fixes the Low Battery Resound at 24 hours for fire points.
RPS Menu Location
SDI2 Modules > Wireless Receiver > Low Battery Resound

15.6.5 Enable Jamming Detection

Default: Yes
Selections:
– Yes - enable RF jamming (interference) detection.
– No - disable RF jamming (interference) detection.

For the B820 Inovonics Wireless module, RF jamming (interference) detection is always enabled, even when this parameter is set to No.

RPS Menu Location

SDI2 Modules > Wireless Receiver > Enable Jamming Detection

15.7 Wireless Repeater

Wireless repeaters are not physically connected to the SDI2 bus. You must configure a wireless interface module as part of the system.

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. Choose the type of wireless receiver before you configure any repeaters. The control panel supports up to 8 repeaters simultaneously. All repeaters must be the same type.

15.7.1 Module Enclosure Tamper

Default: No - Disable

Selections:

– Yes - enable enclosure tamper input
– No - disable enclosure tamper input

When the tamper input is enabled, the control panel creates a tamper event when the enclosure is opened, or when the enclosure is removed from the wall.

RPS Menu Location

SDI2 > Wireless Repeater > Enclosure Tamper

15.7.2 RADION RFID (B810)

Default: 0

Selection: 0, 11 - 167772156

The Radio Frequency device Identification number (RFID) is a unique number assigned to a wireless devices at the factory. The RFID number is located on the product label.

Since wireless repeaters are both receivers and transmitters they are assigned an RFID.

RPS Menu Location

SDI2 Modules > Wireless Repeater > RFID (B810 RADION Wireless)

15.7.3 Inovonics RFID (B820)

Default: N/A

Range: 0 - 99999999

The Radio Frequency device Identification number (RFID) is a unique number assigned to a wireless devices at the factory. The RFID number is located on the product label.

Since wireless repeaters are both receivers and transmitters they are assigned an RFID.

RPS Menu Location

SDI2 Modules > Wireless Repeater > RFID (B820 Inovonics Wireless)

16 Hardware switch settings

16.1 Keypad address

B91x Basic Keypad address switch settings

Address	Switches					
	1	2	3	4	5	6
1	ON	OFF	OFF	OFF	OFF	OFF
2	OFF	ON	OFF	OFF	OFF	OFF
3	ON	ON	OFF	OFF	OFF	OFF
4	OFF	OFF	ON	OFF	OFF	OFF
5	ON	OFF	ON	OFF	OFF	OFF
6	OFF	ON	ON	OFF	OFF	OFF
7	ON	ON	ON	OFF	OFF	OFF
8	OFF	OFF	OFF	ON	OFF	OFF
9	ON	OFF	OFF	ON	OFF	OFF
10	OFF	ON	OFF	ON	OFF	OFF
11	ON	ON	OFF	ON	OFF	OFF
12	OFF	OFF	ON	ON	OFF	OFF
13	ON	OFF	ON	ON	OFF	OFF
14	OFF	ON	ON	ON	OFF	OFF
15	ON	ON	ON	ON	OFF	OFF
16	OFF	OFF	OFF	OFF	ON	OFF
17	ON	OFF	OFF	OFF	ON	OFF
18	OFF	ON	OFF	OFF	ON	OFF
19	ON	ON	OFF	OFF	ON	OFF
20	OFF	OFF	ON	OFF	ON	OFF
21	ON	OFF	ON	OFF	ON	OFF
22	OFF	ON	ON	OFF	ON	OFF
23	ON	ON	ON	OFF	ON	OFF
24	OFF	OFF	OFF	ON	ON	OFF
25	ON	OFF	OFF	ON	ON	OFF
26	OFF	ON	OFF	ON	ON	OFF
27	ON	ON	OFF	ON	ON	OFF
28	OFF	OFF	ON	ON	ON	OFF
29	ON	OFF	ON	ON	ON	OFF

Address	Switches					
	1	**2**	**3**	**4**	**5**	**6**
30	OFF	ON	ON	ON	ON	OFF
31	ON	ON	ON	ON	ON	OFF
32	OFF	OFF	OFF	OFF	OFF	ON

B92x Two-line Keypad / B93x ATM Style Keypad address switch settings
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 figure below shows the address switch setting for address 1.

B94x Touch Screen Keypad address switch settings
To set the address, use the up and down arrows on the right of the switches image to change the ones digit, and the arrows on the left to change the tens digit. Press the diagonal arrow under the switches to save the setting and return to the power up screen.

16.2 B208 Octo-input Module 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.
Terminate unused B208 inputs with an EOL resistor.

16.3 B308 Octo-output Module switch settings

This table describes the relationship between the module switch settings and the output number range that corresponds to the setting.

16.4 B426 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
1	1	SDI2	Automation, remote programming, reporting

16.5 B450 Cellular Module switch settings

This table describes the relationship between the module switch settings and type of control panel communication that corresponds to the setting.

B450 switch setting	Address	Bus type	Function
0	-	-	local configuration setting
1	1	SDI2	Automation, remote programming, reporting

16.6 B5xx Aux Power Supply switch settings

The rotary address switch range for the B5xx Aux Power Supply is between 1 and 4 for the B6512 and the B5512, between 1 and 2 for the B4512, and between 1 and 2 for the B3512 control panels. Address ranges 00 and 05-99 are not valid on the SDI2 device bus. The factory default setting is 01. When using more than one power supply, assign each power supply a different switch setting.

Valid B5xx switch settings
01
02
03
04

16.7 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.

16.8 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 these control panels.

16.9 B901 Access Module switch settings

Two address switches determine the address for the B901 Access Control Module. The control panel uses the address for communications.
Use a slotted screwdriver to set the address switches.

Address	Designation
0,0	Disabled
0,1 to 0,4	Doors 1 through 4

17 Configuring for Cellular Service

Sign-up for Bosch Cellular Service first

Before you can utilize cellular communication for reporting, personal notifications, RPS connections, or RSC connections you need to contact your regional Bosch technical support to set up or get your Account Details.

Configure RPS for cellular service

Configuring RPS for cellular service is quick and easy using the Configuration Assistant:

1. Click Config to open the Configuration menu.
2. Select Open Configuration Assistant.

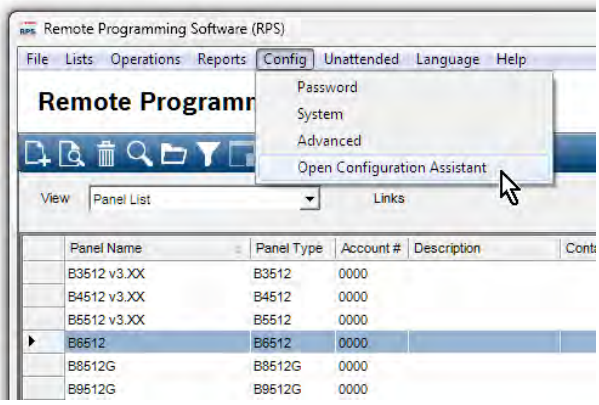


Figure 17.1:

Manual RPS Configuration for Cellular Service

If you choose not to use not to use the Configuration Assistant, use these steps to configure RPS for cellular service:

1. Click Config to open the Configuration menu, and then select System.
2. Click the Connectivity tab.
3. Click Cellular.
4. RPS will attempt to use ICCID information to automatically create a VPN connection to the panel when using a cellular module. If your cellular service details cannot be automatically retrieved and require a manual VPN connection set up, enter the connection details into the VPN tab. RPS will use that VPN information to automatically create your Windows VPN during each panel connection and then delete it when disconnecting.

Configure the control panel account for cellular service

Configuring a control panel account for cellular service is quick and easy using the Account Assistant:

1. In the Panel List, right-click the panel account you want to configure for cellular service.
2. Select Open Account Assistant.

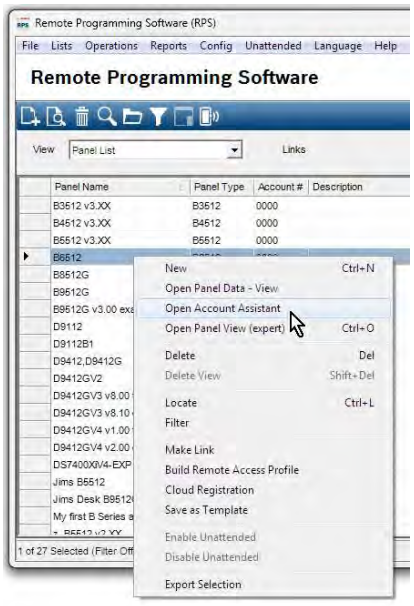


Figure 17.2:

If you choose not to use not to use the Account Assistant, you can manually configure a control panel account for cellular service using these steps:

1. In the Panel List, right-click the panel account you want to configure for cellular service, then select Open Panel Data - View.
2. Click the Cellular tab.
3. Enter information in the Cellular Connectivity fields. RPS will use the ICCID number to retrieve and store the assigned IP address, phone number and assigned plan for use during connections.

– When connecting to this panel using Cellular, RPS will retrieve the service details needed to automatically create your Windows VPN, establish the panel connection and then automatically remove the Windows VPN after disconnecting from the panel.

– If your cellular service requires a manual VPN connection set up for Cellular connections, enter the connection details into the RPS System Configuration > Connectivity > VPN tab. RPS will use that VPN information to automatically create the Windows VPN during each panel connection and then delete it when disconnecting.

4. Click OK when finished.
5. Set panel parameters by right-clicking the panel account you clicked in step 1, then select Open Panel View.
6. Panel Wide Parameters > *Cellular Plug-in Module, page 38*: leave the parameters here at their defaults. Only change for UL1610 commercial listed installations requiring low signal notification.
7. Panel Wide Parameters > *Communicator, overview, page 63* > Primary Destination Device (Backup Destination Device): to send reports for a Route Group via a cellular communicator, select a (Plug-in) Cellular Destination as the Primary (or Backup) Destination.
8. Panel Wide Parameters > *Enhanced Communication, page 68*: set reporting Destinations, and polling/supervision settings here. Make sure that cellular polling rates follow recommended settings and align with your cellular plan.
9. Panel Wide Parameters > Personal Notification > *Personal Notification Destinations, page 89*: set phone numbers for SMS messages, email addresses for email messages. Set Method to Plug in Cellular SMS, Bus Device Cellular SMS, Plug in Cellular Email, or Bus Device Email.

Refer to

- *Cellular Plug-in Module, page 38*
- *Communicator, overview, page 63*
- *Enhanced Communication, page 68*
- *Personal Notification Destinations, page 89*

18 IP Address and Domain Name formats

IPv4 Address Format

IPv4 addresses are in ASCII decimal format, xxx.xxx.xxx.xxx (xxx = 0 to 255). The four octets (xxx) of the address are separated by periods.

Correct: 12.3.145.251

Incorrect: C.17.91.FB

IPv6 Address Format

IPv6 addresses consist of eight groups of 4 hexadecimal digits separated by colons, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, x = 0 to F.

Fully Qualified Domain Name Format

The fully qualified domain name defines the exact address of a device in the Domain Name System (DNS) 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 letters (A-Z), numbers (0-9), and the minus sign (-) are allowed in the text labels in 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 DNS servers available to the IP communicator. This can be verified using a ping tool.

Additional Information

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

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life

202409111634