Easy Series (ICP-EZM2)

EN

Installer Guide

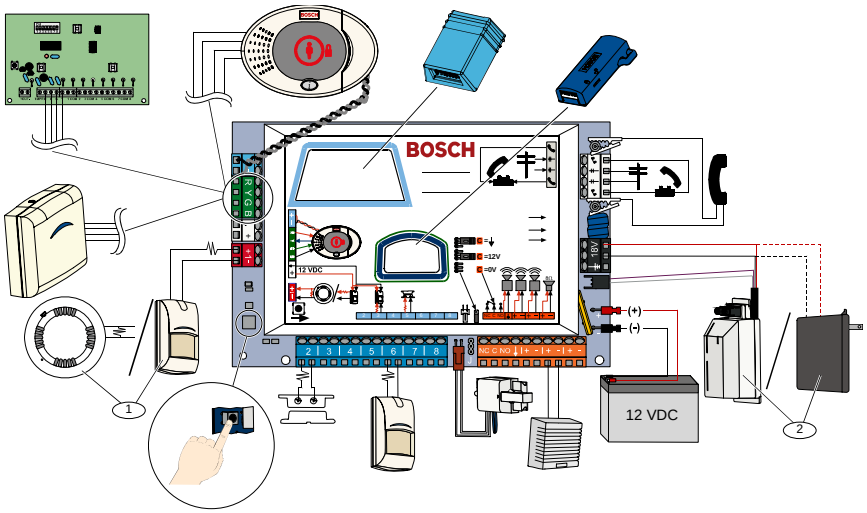
Intrusion Control Panel

BOSCH

Contents

1.0 Quick Reference

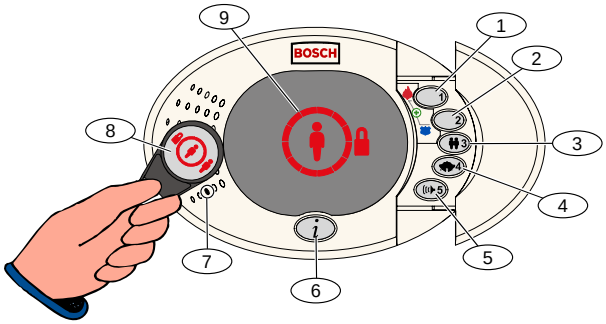
1.1 System Overview



[1] Connect either a two-wire smoke detector or an intrusion detector, such as a motion detector, to Point 1.

[2] Use either the EZPS wire-in power supply or a transformer.

1.2 Control Center Overview



Callout	Description
1	Press and hold [1] for two sec to start a fire alarm. For an emergency alarm, press and hold [1] and [2] for two sec.
2	Press and hold [2] for two sec to start a panic alarm. For an emergency alarm, press and hold [1] and [2] for two sec.
3	Press and hold [3] for 2 sec to enter User Menu, and then present token or enter passcode. Select an option[1]: • **Add User:** Press [1]. Use this option to add a new user. You must assign a passcode. You can also record a description and assign a token or key fob. Follow all voice prompts. • **Change User:** Press [2]. Use this option to add or change the passcode, description, token, or key fob assigned to an existing user. Follow all voice prompts. • **Delete User:** Press [3].
4	Press and hold [4] for 2 sec to turn Chime Mode on or off.
5	Press and hold [5] for 2 sec to enter Volume Menu, and then press again to select a level: low, medium, high, or quiet[2].
6	Press [i] to turn the system on or off. Follow all voice prompts.
7	Speak into the audio interface to talk to someone on the telephone during a two-way voice session.
8	Present token to control center to turn the system on or off.
9	Control center display. Refer to *Section 7.5 Display States* on page 62 for more information.

[1] Master user token or passcode required to access these options. Other users can change only their own passcodes.

[2] Quiet Control Center: Exit Delay and Entry Delay tones are silenced.

1.3 Basic Operation Information

Item	Description	
Start and end a phone session	**House phone:**	Press [#] three times, and enter a passcode.
	Outside phone:	Dial the house phone number, and press [*] three times when the call is answered. Enter a passcode.
	Installer quick connect:	Connect a test telephone to the control panel's test posts or telephone terminals. Press and hold the system test button for approximately 15 sec. Enter a passcode.
	End a phone session:	Press [#] repeatedly until the system says "goodbye."
Enter and exit programming	Start a phone session (refer to options above). Enter installer passcode when prompted. From the Installer Menu, press [3] for basic programming, or [4] for expert programming. - For Basic Programming, refer to *Section 4.2* on page 30. - For Expert Programming, refer to *Section 4.3* on page 36. To exit programming, press [#] repeatedly until you hear the system announce the Installer Menu options.	
Passcode length	Options are four digits or six digits. Selection affects all passcode lengths. Expert programming →*Expert Programming Item Number 861*.	
Installer passcode	Four-digit default = 5432; six-digit default = 543211 (*Expert Programming Item Number 7011*).	
Master user passcode	Four-digit default = 1234; six-digit default = 123455. (*Expert Programming Item Number 7001*).	
Factory default	In expert programming, enter *Expert Programming Item Number 9999*. Doing this restores all factory default values. All programming items, except for the country code, are reset when you restore the factory default values. All recorded speech items are unaffected.	
Add or change users	Start a phone session, or press and hold [3] on the control center (refer to *Section 1.2 Control Center Overview* on page 3). Enter the master user passcode. Press [4] to select the User Menu. Press [1] to add a new user, or press [3] to change an existing user. Follow all voice prompts. When you add a new user or change an existing user, you can also assign a token or key fob.	
System Test	On the control panel board, press the System Test button once to start the System Test.	
"Call for Service" Details	Enter the installer passcode when you hear the "Call for Service" message. The system announces the system trouble condition and then asks you to select a menu option.	

1.4 System Setup (Wired and Wireless)

After the system is installed and configured, add key fobs when you add users.

Wireless support is not investigated by UL.

To install an Easy Series Intrusion Control Panel with wireless devices:

1. Follow all instructions in the *wLSN Reference Guide* (P/N: F01U009440) to verify adequate signal strength exists at each device location.
2. Install all hard-wired devices, such as the control panel, control center, input and output devices, DX2010 Input Expanders, and the wireless hub.
   Refer to the installation instructions supplied with each device for specific installation and configuration instructions.

The control panel assigns wireless point numbers based on whether or not one or more DX2010 Input Expanders are connected to the control panel.

3. Install the bases for all wireless devices.
4. Apply power to the control panel.
5. Start the System Test:
   - **From Phone:**
     1. Start a phone session.
        Refer to *Section 1.3 Basic Operation Information* on page 4 for instructions.
     2. From the Installer Phone Menu, press [1] for System Maintenance.
     3. Press [2] for Full System Test.
        Refer to *Section 1.5 Installer Phone Menu* on page 6.
   - **From Control Panel:** To start the full system test, press and hold the System Test button for one second. Refer to *Section 5.0 System Test* on page 56 for more information.
6. When the system announces "Install all batteries," install the batteries or remove the battery tabs from all wireless devices. Mount the device covers on the bases.
7. When all batteries are installed and device covers are mounted, press [1] on the phone or control center to continue.
   The system identifies (discovers) new wireless devices on the system. This process takes up to 4 min to complete. When the discovery process is complete, the system announces the number of devices discovered.
8. When the system announces "Test all points," test each device (fault and restore), including wireless inputs and outputs.
   Refer to *Section 3.1.4 Test Devices* on page 24 for more information.

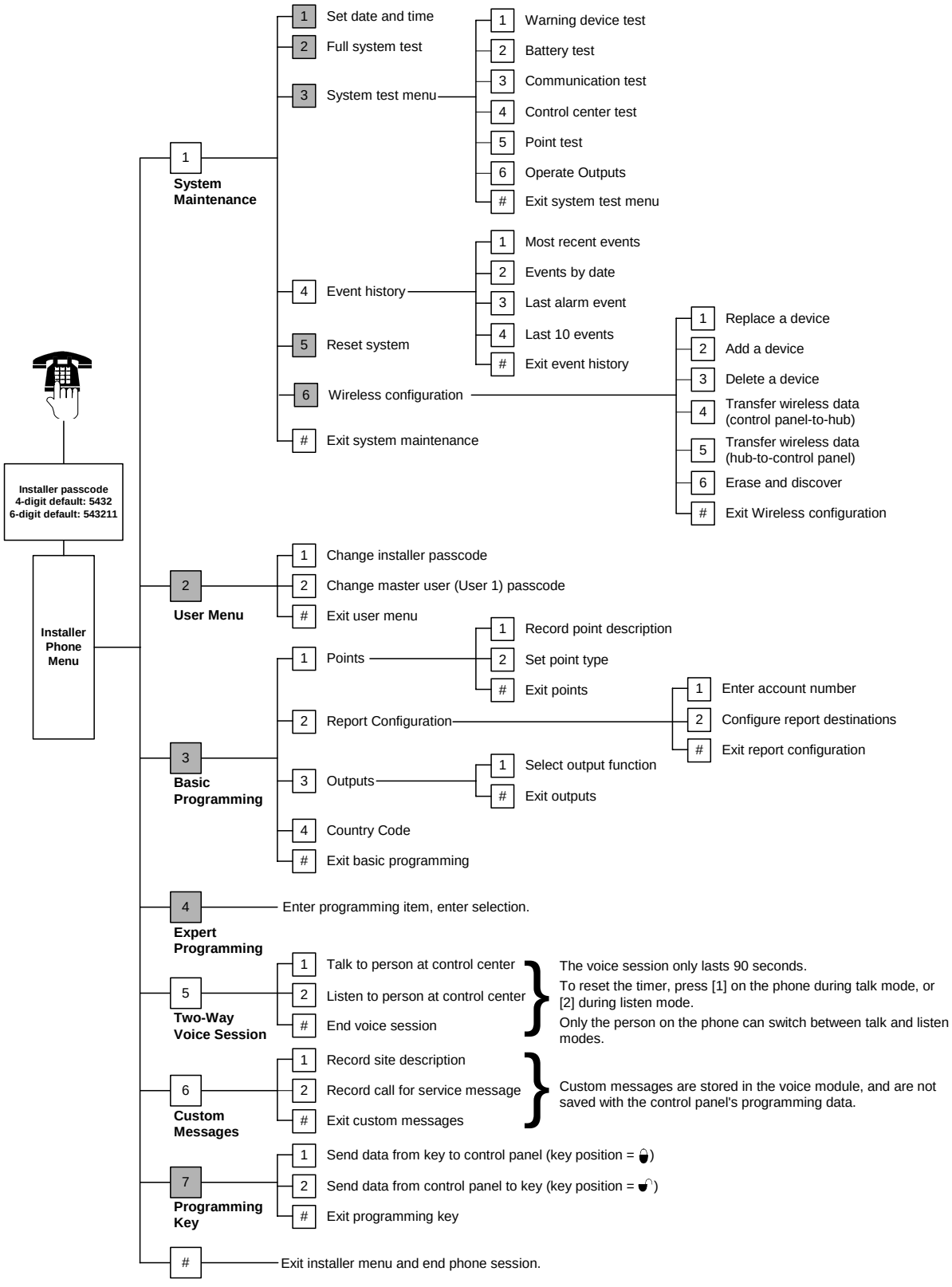
Point numbers are assigned to wireless devices in the order that the devices are tested (tampered or faulted and restored). If specific point numbers are preferred for wireless devices, ensure that the wireless devices are tested in the appropriate order. Otherwise, the system assigns the lowest available point number to the first tested wireless device.

9. As you test each device, complete *Section 4.3.5 Point Programming Items* on page 46, and *Section 4.3.6 Output Programming Items* on page 51.
   When you restore the device, the system announces the assigned device number.

   Complete *Sections 4.3.5* and *4.3.6* as you test the inputs and outputs. Otherwise, you cannot cross-reference point numbers to point descriptions in the event of a point trouble.

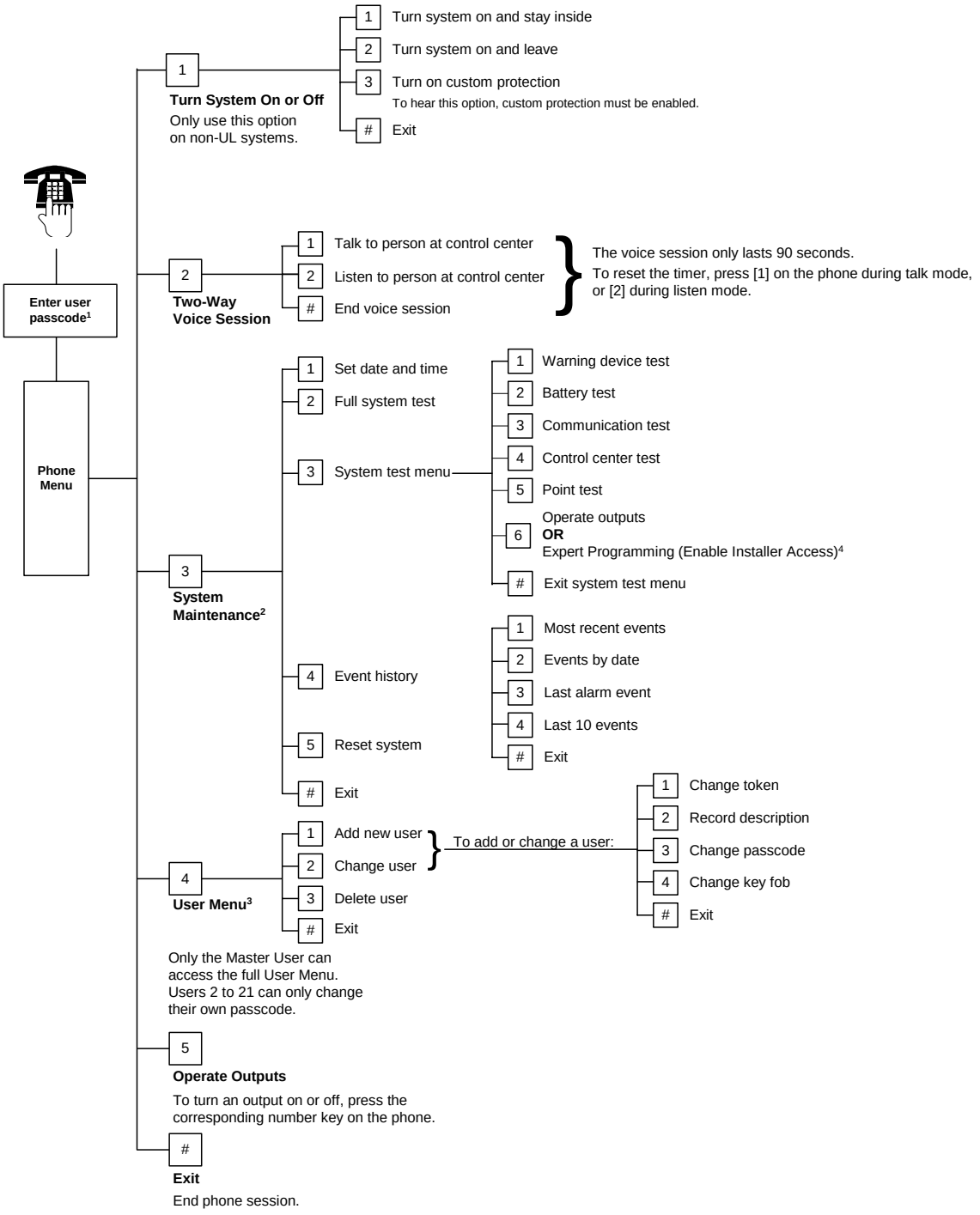
   The control panel completes the remaining system tests and notifies you when they are complete.
10. When the control panel completes all system tests, enter **Basic Programming**. You can also use RPS to program the control panel.

1.5 Installer Phone Menu



= The system's arming status (on or off) and *Expert Programming Item Number 142's* setting of (0 or 1) determines the availability of these menu items.

1.6 User Phone Menu



[1] Only a user passcode (Users 1 to 21) can access the User Menu.

[2] If the system is on, the System Maintenance option is not available.

[3] Only the master user can add, change, or delete users. Users 2 to 21 can only change their own passcodes. User voice descriptions are stored in the voice module and are not transferred to the control panel with programming data.

[4] Option 6 allows the master user (User 1) to enable the Installer Passcode. Refer to *Expert Programming Item Number 142* on page 39 for more information.

Availability of the menu items shown above depends on the system's status.

2.0 Installation

Only use authorized service personnel to install this system.

Because the control panel is permanently connected equipment, a readily accessible disconnect device must be included into the building installation wiring.

Follow anti-static procedures when handling the control panel board.

Touch the earth ground terminal on the control panel board to discharge any static charge before working on the control panel board.

To aid in system installation, this section is divided into sub-sections and labeled in a step-by-step format. Each sub-section, or major step, might consist of several minor steps that must be completed before proceeding to the next sub-section or major step.

2.1 Enclosure Installation (Step 1)

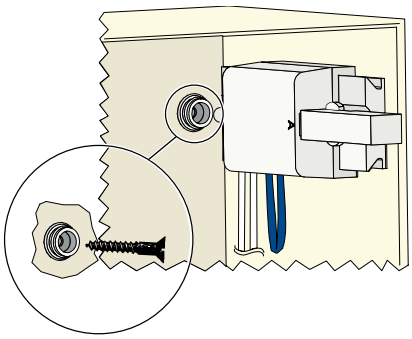
Use proper anchor and screw sets when installing the enclosure on non-load-bearing surfaces, such as drywall.

1. Mount the optional EZTS Tamper Switch.

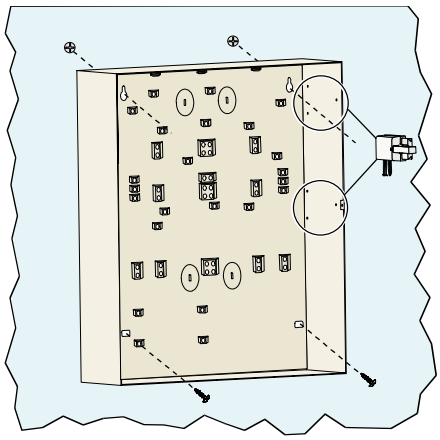
   If a wall tamper is required, insert the round plastic wall plug before mounting the enclosure.

   Refer to the *EZTS Cover or Wall Tamper Switch Installation Guide* (P/N: F01U003734) for complete installation instructions.

   Refer to *Programming Item 137* on page 39 for enclosure tamper options.

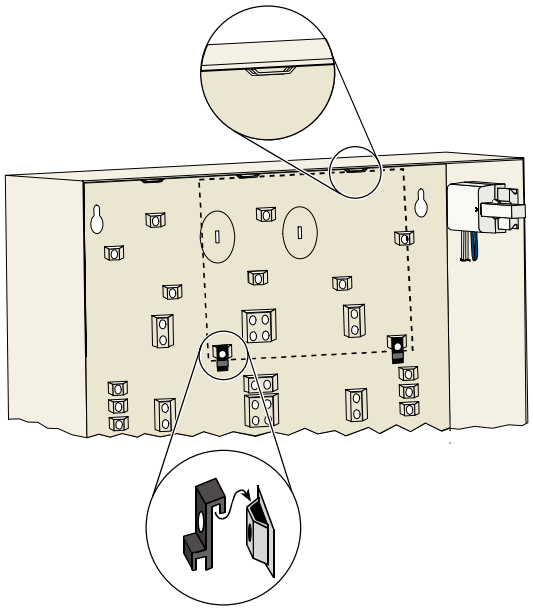


2. Mount the enclosure. Screws not supplied.

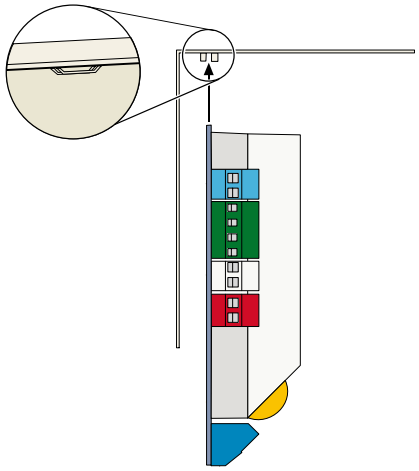


2.2 Control Panel Board Installation (Step 2)

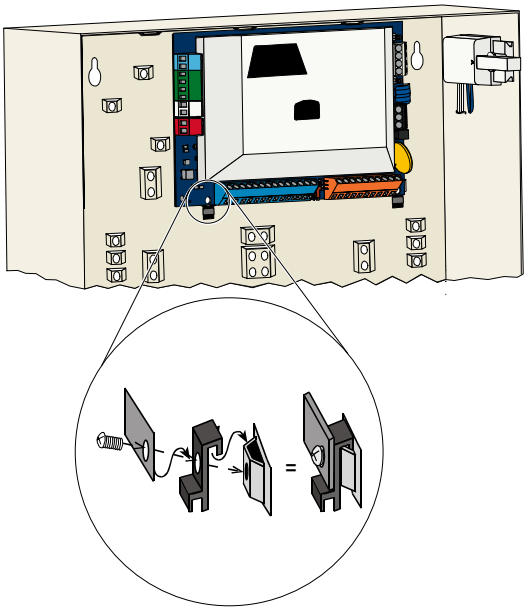
1. Place the mounting clips on the enclosure standoffs.



2. Place the top edge of the control panel board between the enclosure retaining slots, and then set the control panel board on the mounting clips.



3. Secure the control panel board to the mounting clips using the supplied screws.



2.3 Control Center Installation (Step 3)

For complete control center installation instructions, refer to the *EZ1 Control Center Installation Guide* (P/N: F01U003737) included with the control center.

To ensure proper RF ID reader operation, mount the control center only on a non-metallic surface.

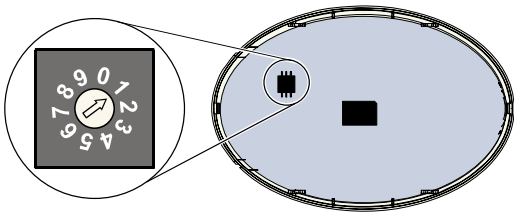
If you install more than one control center, ensure that there is at least 1.2 m (4 ft) of space between each control center.

1. Set the address on the control center.

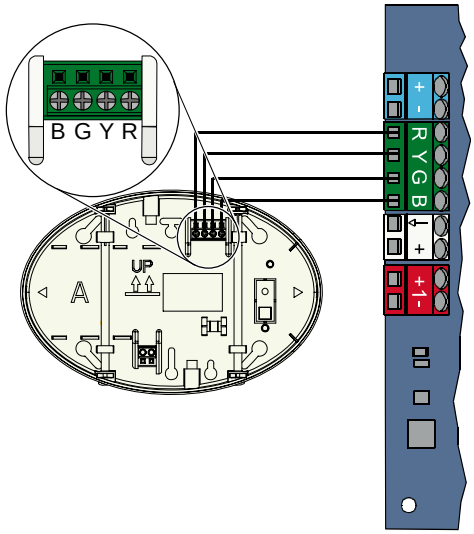
   The control panel supports up to four control centers.

   Each control center must have a different address. Valid addresses are 1 to 4.

   The address switch is located on the inside of the control center.



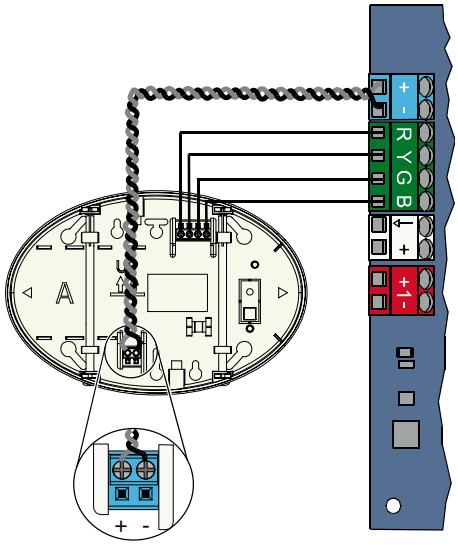
2. Connect the control center data bus terminals to the control panel data bus terminals.



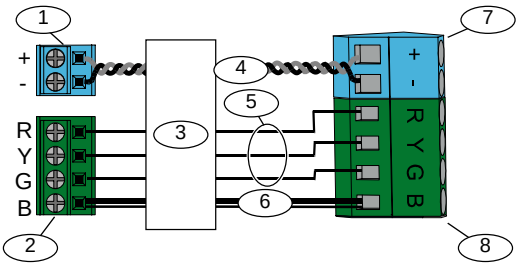
3. Connect the control center audio bus terminals to the control panel audio bus terminals.

   Twisted pair wiring is recommended for audio bus connections.

   If CAT5 cable is used, refer to the following CAT5 figure.



CAT5 Cable Connections



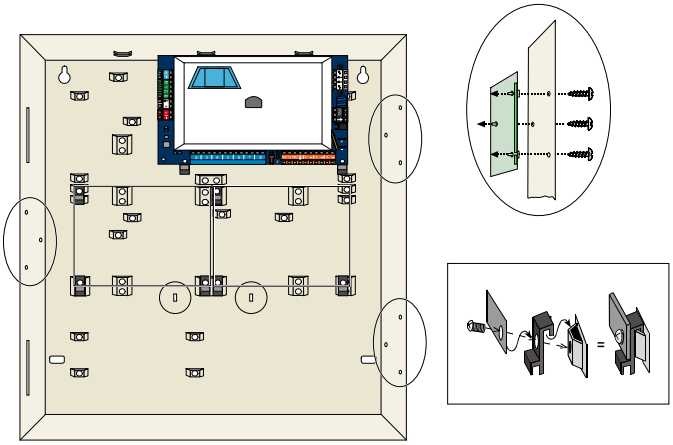
1 - Control center audio bus terminals
2 - Control center data bus terminals
3 - CAT5 cable
4 - Blue and blue-and-white-striped conductors (twisted pair)
5 - Solid color conductors
6 - White striped conductors
7 - Control panel board audio bus terminals
8 - Control panel board data bus terminals

2.4 DX2010 Installation (Step 4)

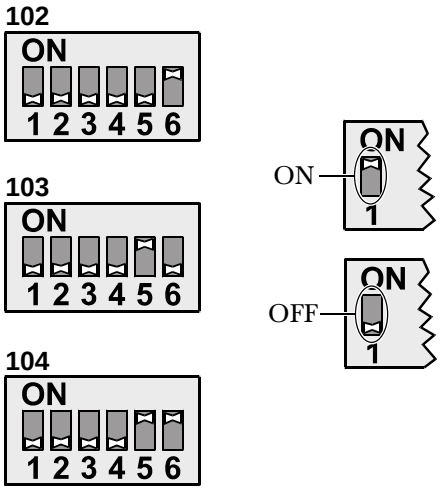
The control panel supports up to three DX2010 Input Expanders for Points 9 to 32.

Refer to the *DX2010 Installation Instructions* (P/N: 49533) for more information.

1. Mount the DX2010 into the control panel's enclosure, or other suitable enclosure.



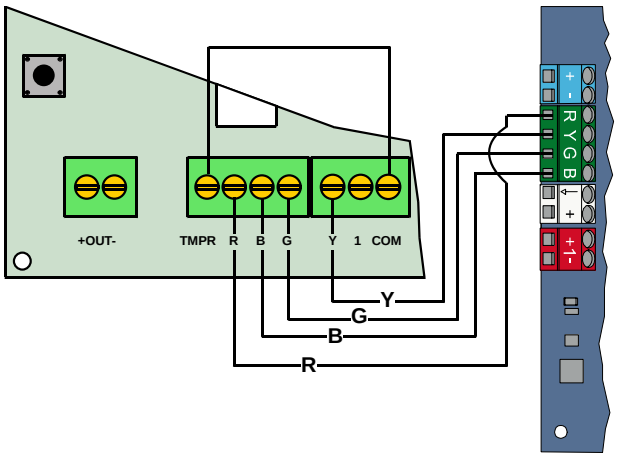
2. Set the DX2010's DIP switches.
   - Points 9 to 16 = Address 102
   - Points 17 to 24 = Address 103
   - Points 25 to 32 = Address 104



3. Connect the DX2010 to the control panel.

   Connect a wire jumper to the TMPR and COM terminals to disable the DX2010's tamper input.

   For point wiring options, refer to *Section 2.6 Supervised Point Connections* on page 14.



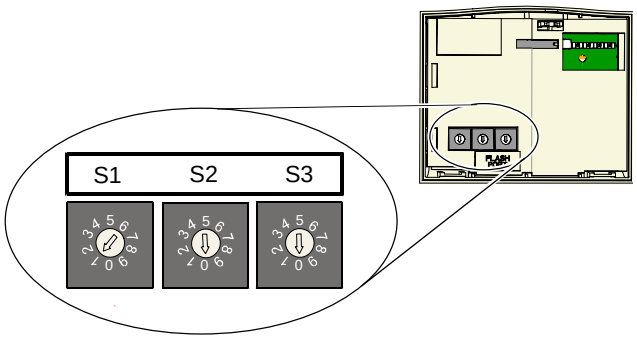
2.5 Wireless Hub Installation (Step 5)

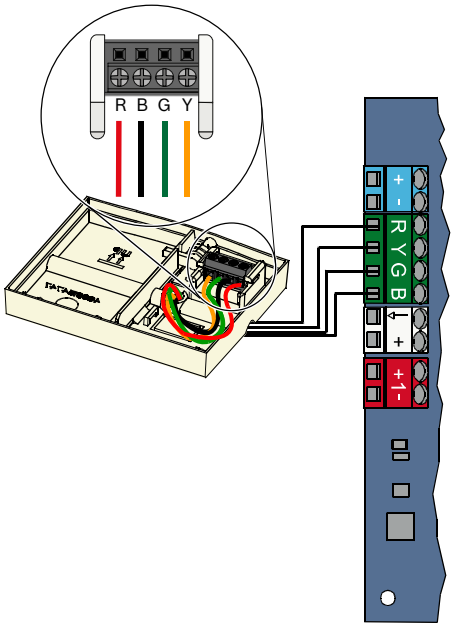
Before installing the wireless hub or any wireless devices, refer to *Section 3.0 Point Expansion* on page 23, the *ISW-BHB1-WX Installation Instructions* (P/N: F01U500915), the *wLSN Reference Guide* (P/N: F01U009440), and the installation instructions supplied with each wireless device.

1. Perform a site test as described in the *wLSN Reference Guide*.
2. Set the S1 switch on the wireless hub to Address 50 (Position 1).

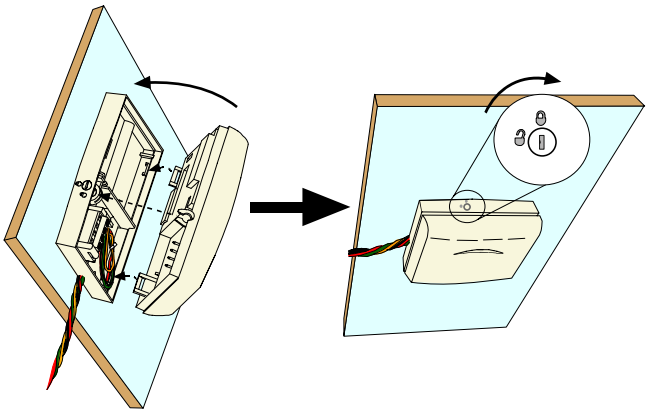
   The control panel supports one wireless hub.

   Switches S2 and S3 are not used for device addressing.





3. Connect the hub to the control panel.



4. Put the cover on the wireless hub and lock the cover to the hub.
5. Install the wireless device bases as described in their installation instructions.

2.6 Supervised Point Connections (Step 6)

Separate primary AC power and standby battery wires from all power-limited wiring. Refer to *Section 7.2 Power-limited Wire Routing* on page 58 for more information.

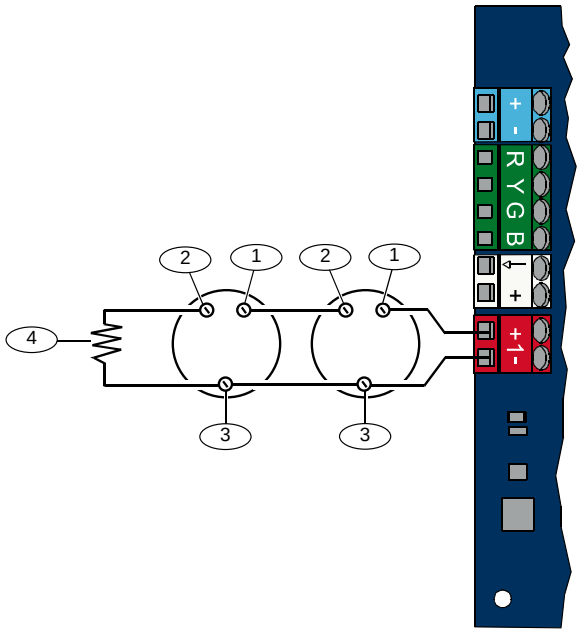
2.6.1 Fire Point Wiring

Supervised Point 1 supports two- and four-wire smoke detectors.

Supervised Points 2 to 32 support only four-wire smoke detectors.

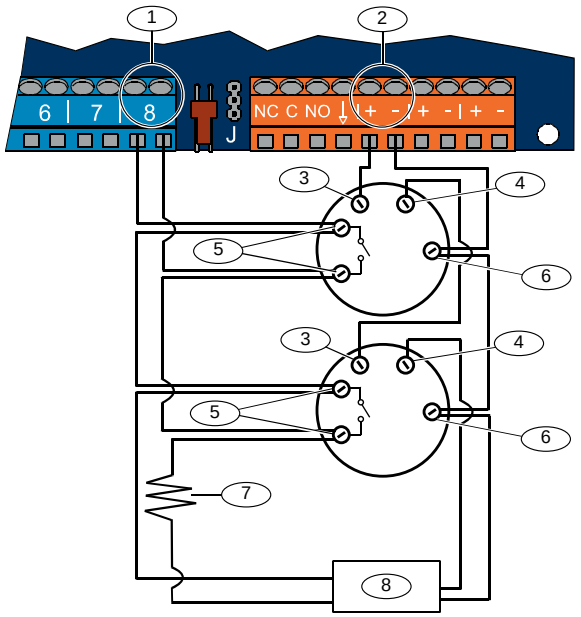
To program supervised points as fire points, refer to *Section 4.2.1 Points* on page 31.

For intrusion point configuration, refer to *Section 2.6.2 Intrusion Point Wiring* on page 15.



Two-wire smoke detector wiring

1 - Power-in terminal
2 - Power-out terminal
3 - Common (negative) terminal
4 - 2.2 k Ω end-of-line resistor (P/N: 25899)



Four-wire smoke detector wiring

1 - Supervised Points 1 to 32 (Point 8 shown in figure)
2 - Programmable Output (PO) (PO 2 shown in figure)
3 - Power-in terminal
4 - Power-out terminal
5 - Alarm terminals
6 - Common (negative) terminal
7 - End-of-line resistor (P/N: 25899)
8 - Bosch EOL200 End-of-Line Module

Refer to the *Easy Series Smoke Detector Compatibility List* (P/N: F01U004853) for compatible two-wire smoke detectors.

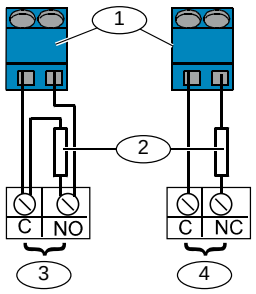
When using an output to supply power to a four-wire smoke detector, program the output function for System Reset. Refer to *Section 4.2.3 Outputs* on page 33.

2.6.2 Intrusion Point Wiring

Refer to the figures below to wire Supervised Points 1 to 32 as wired or wireless intrusion points.

To program Supervised Points 1 to 32 as intrusion points, refer to *Section 4.2.1 Points* on page 31.

For fire point configuration, refer to *Section 2.6.1 Fire Point Wiring* on page 14.



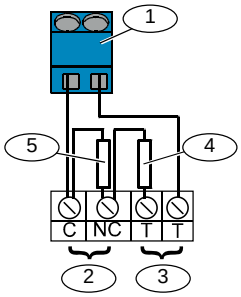
Single 2.2 kΩ EOL resistor

1 - Supervised point (on-board, DX2010, or wireless input)

2 - 2.2 kΩ EOL resistor

3 - Alarm terminals (Normally Open)

4 - Alarm terminals (Normally Closed)



Dual 2.2 kΩ Resistors (Point Tamper*)

1 - Supervised point (on-board, DX2010, or wireless input)

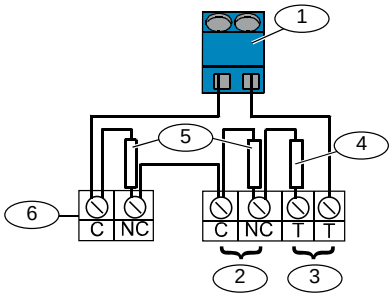
2 - Alarm terminals (Normally Closed)

3 - Tamper terminals (Normally Closed)

4 - 2.2 kΩ EOL resistor

5 - 2.2 kΩ alarm resistor

** This option is not allowed by UL.*



Dual 2.2 kΩ Resistors (Point Tamper*)

1 - Supervised point (on-board, DX2010, or wireless input)

2 - Alarm terminals (Normally Closed)

3 - Tamper terminals (Normally Closed)

4 - 2.2 kΩ end-of-line resistor

5 - 2.2 kΩ alarm resistor

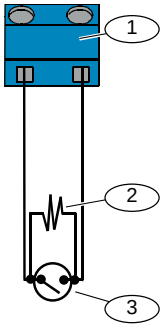
6 - Additional devices (up to 4 maximum)

** This option is not allowed by UL.*

2.6.3 Keyswitch Wiring

Refer to the figure below to wire Supervised Points 1 to 32 as keyswitch points (Point 2 shown in figures).

To program Supervised Points 1 to 32 as keyswitch points, refer to *Section 4.2.1 Points* on page 31.

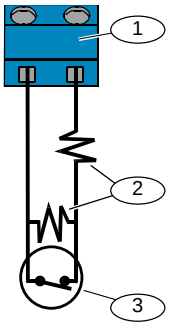


Single 2.2 kΩ end-of-line resistor option

1 - Supervised point (on-board, DX2010, or wireless device)

2 - 2.2 kΩ resistor

3 - Normally-open momentary or maintained keyswitch



Dual 2.2 kΩ resistors (point tamper option)

1 - Supervised point (on-board, DX2010, or wireless device)

2 - 2.2 kΩ resistor

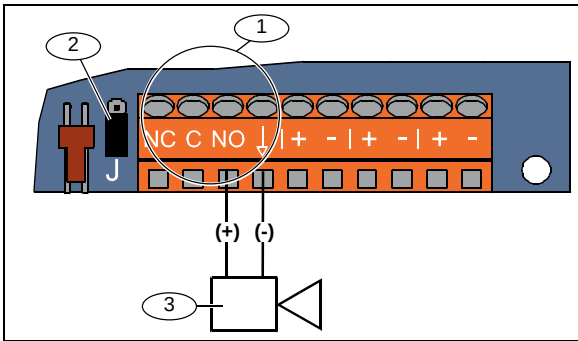
3 - Normally-closed momentary or maintained keyswitch

2.7 Programmable Output Connections (Step 7)

Separate primary AC power and standby battery wires from all power-limited wiring. Refer to *Section 7.2 Power-limited Wire Routing* on page 58 for more information.

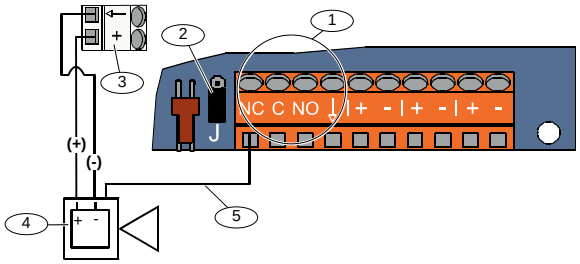
2.7.1 Programmable Output 1 Wiring

Switched 12 V Option



Warning device (without battery)

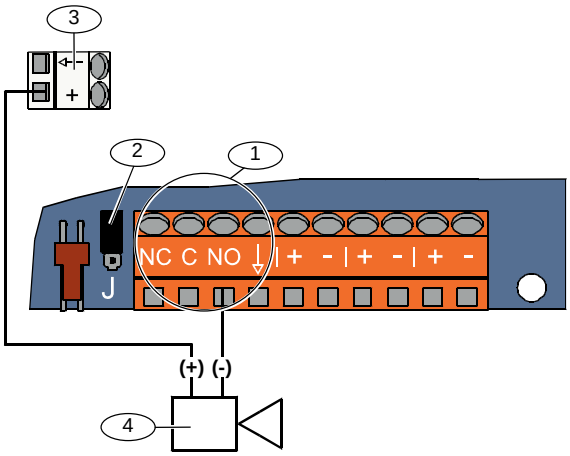
1 - Programmable Output 1 (PO 1)
2 - Jumper plug position for switched 12 V option
3 - Warning device



Warning device (with battery)

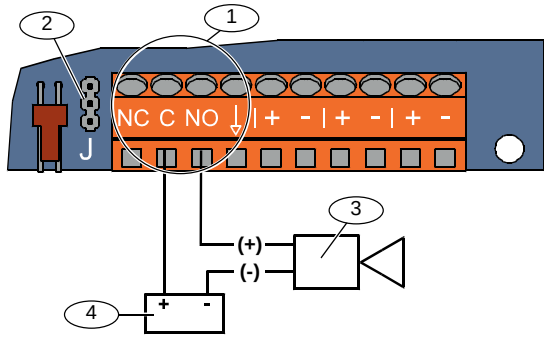
1 - Programmable Output 1 (PO 1)
2 - Jumper plug position for switched 12 V option
3 - Control panel board white auxiliary power terminals (12 VDC)
4 - Warning device
5 - Warning device activates when trigger voltage is removed

Switched Ground Position



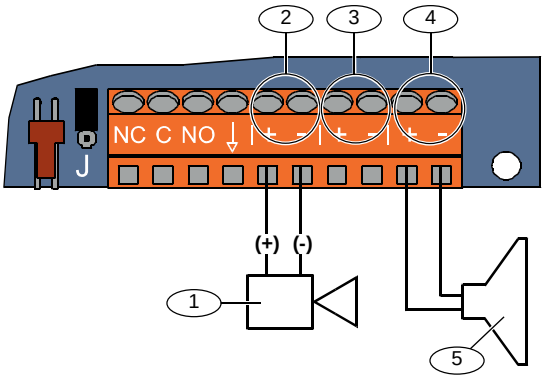
1 - Programmable Output 1 (PO 1)
2 - Jumper plug position for switched ground option
3 - Control panel board white auxiliary power terminals (12 VDC)
4 - Warning device

Dry Contact Option



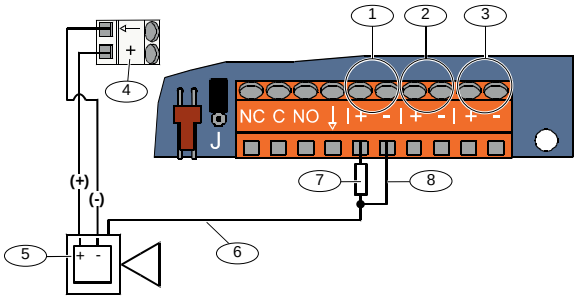
1 - Programmable Output 1 (PO 1)
2 - Jumper plug position for dry contact option (no jumper)
3 - Warning device (normally-open option)
4 - Power source

2.7.2 Programmable Outputs 2 to 4 Wiring



Warning device (without battery)

1 - Warning device (PO 2, 3, or 4)
2 - Programmable Output 2 (PO 2)
3 - Programmable Output 3 (PO 3)
4 - Programmable Output 4 (PO 4)
5 - 8 Ω speaker (PO 4 option only)



Warning device (with battery)

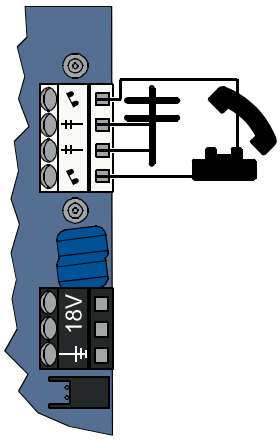
1 - Programmable Output 2 (PO 2)
2 - Programmable Output 3 (PO 3)
3 - Programmable Output 4 (PO 4)
4 - Control panel board white auxiliary power terminals (12 VDC)
5 - Warning device (PO 2, 3, or 4)
6 - Trigger voltage
7 - 10 k Ω resistor
(Refer to warning device instructions for recommended resistor value)
8 - Warning device activates when the programmable output activates

If you program PO 4 as a supervised speaker driver, connect an 8 Ω speaker to prevent speaker supervision troubles. Refer to *Expert Programming Item Number 642* on page 51 for more information.

For a UL-approved installation, only connect a UL listed, 85 dB sounding device to PO 4.

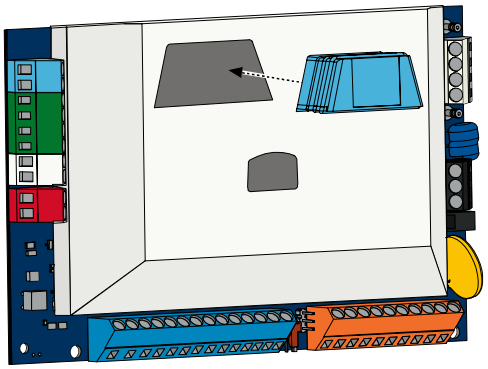
2.8 Phone Line Connections (Step 8)

Connect the incoming phone line and the house phone to the control panel board.



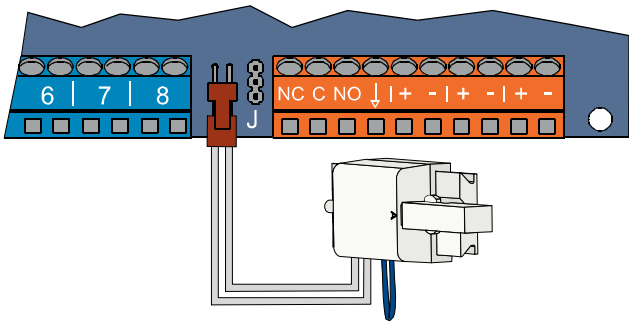
2.9 Insert Voice Module (Step 9)

The voice module is required for system operation.



2.10 EZTS Connections (Step 10)

If the optional EZTS Tamper Switch was installed in *Step 1* on page 8, connect its cable to the two-pin connector on the control panel.



2.11 Power Supply Installation (Step 11)

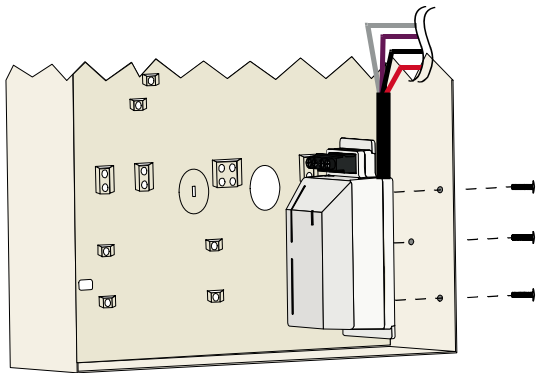
This system uses either the EZPS wire-in power supply, **OR** a plug-in power supply. Both power supplies require the enclosure ground wire and a standby battery.

Follow the instructions below for the power supply used in your installation.

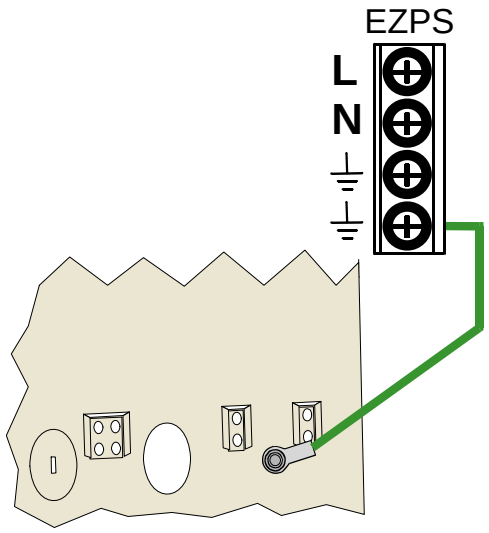
The EZPS is not investigated by UL.

2.11.1 EZPS Wire-in Power Supply

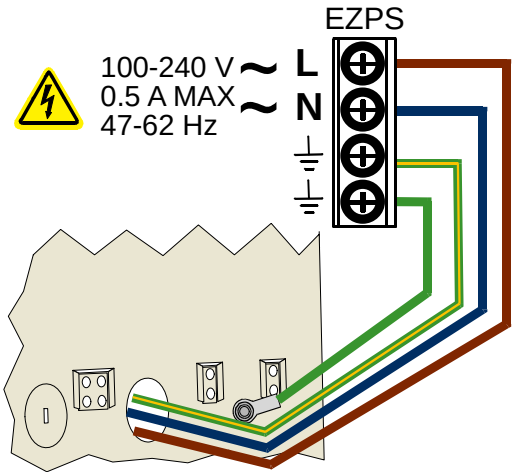
1. Mount the EZPS on the enclosure using the screws supplied with the EZPS.



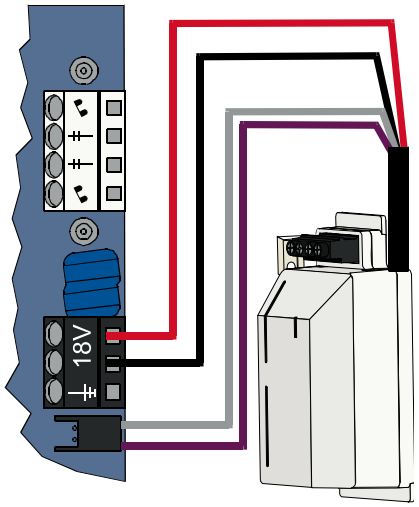
2. Connect the earth ground wire from the EZPS to the enclosure stud.



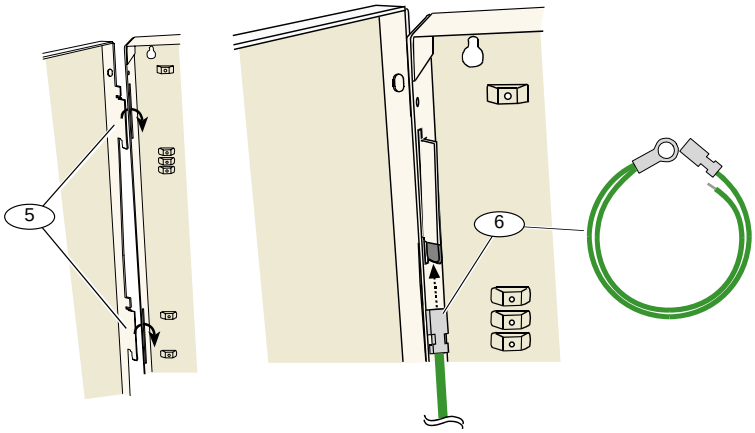
3. Connect AC power to the EZPS.



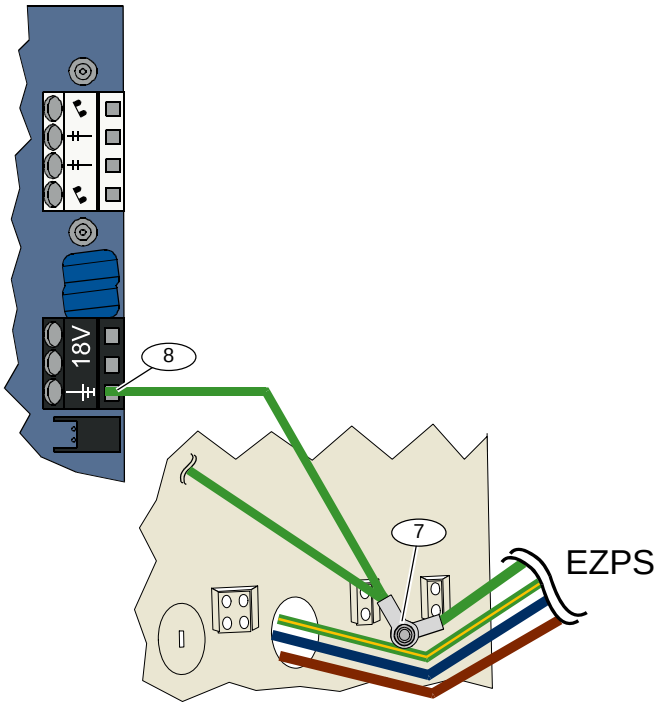
4. Connect the EZPS wires to the control panel board.



5. Insert the door hinges onto the enclosure.
6. Push the enclosure ground wire connector onto the unpainted part of the door's top hinge.

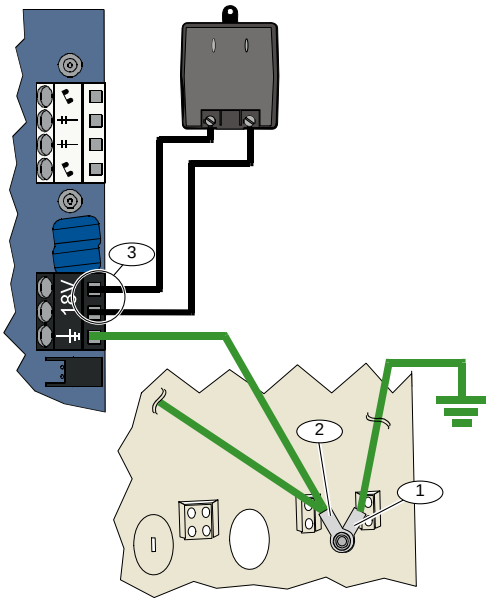


7. Connect the enclosure ground wire to the threaded enclosure stud.
8. Connect the enclosure ground wire to the control panel board's earth ground terminal.



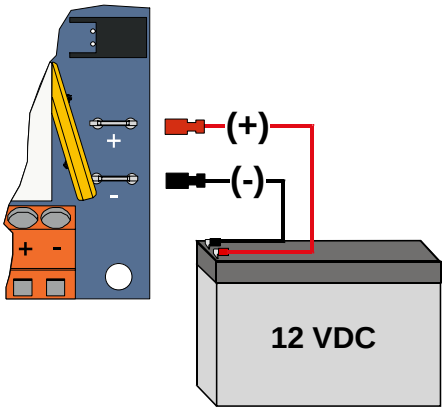
2.11.2 Plug-in Power Supply

1. Connect a ground wire from the enclosure to a good earth ground source.
2. Connect the enclosure ground wire.
   For instructions, refer to *Steps 5* to *8* in *Section 2.11.1 EZPS Wire-in Power Supply* on page 19.
3. Connect the plug-in power supply to the control panel board.



2.11.3 12 VDC Standby Battery

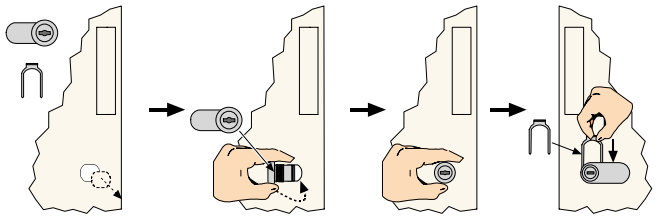
When all system wiring is complete, apply AC and standby battery power to the control panel.



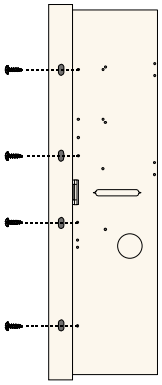
2.12 Secure the Enclosure (Step 12)

To secure the enclosure door:

- Install the enclosure door lock, or
- Secure the door with screws.
  Screws not supplied.



OR



2.13 Program the Control Panel (Step 13)

When installation is complete, you can program the control panel.

Refer to *Section 4.0 Programming* on page 29 for more information.

2.14 Test the System (Step 14)

When programming is complete, you must test the system for proper operation.

Refer to *Section 5.0 System Test* on page 56 for more information.

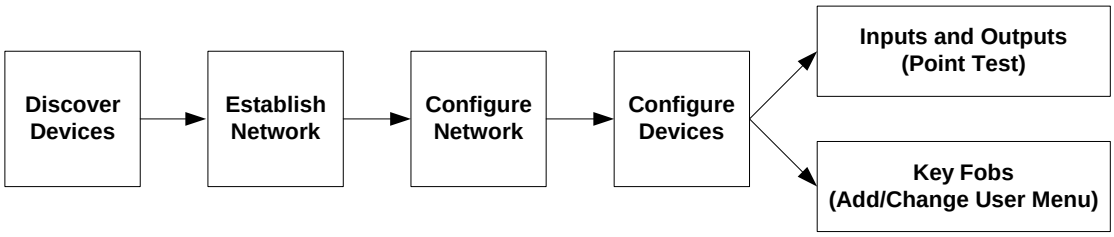
3.0 Point Expansion

For complete wireless installation and configuration information, refer to the *wLSN Reference Guide* (P/N: F01U009440) supplied with the wireless hub, and the installation instructions supplied with each wireless device.

Wireless support is not investigated by UL.

3.1 Establishing the Wireless Network and Configuring Wireless Devices

In order for the wireless network to operate properly, the following process must occur as shown below.



3.1.1 Discover New System

Discovery is the process through which the wireless hub identifies and includes new (undiscovered) devices into the system.

You can only perform the new system discovery process once. To update an existing wireless system, refer to *Section 3.2 Wireless Maintenance* on page 26.

There are three ways to start the discovery process on a new system:

- **System Test Button:**
  1. Ensure that all devices have exited RFSS Mode.
  2. Press and hold the System Test button for one second.
     The device discovery process automatically starts at the beginning of the Point Test.
- **Wireless Configuration Menu:**
  1. Start a phone session.
     Refer to *Section 1.3 System Setup* on page 5 for phone session options.
  2. From the Installer Menu, select System Maintenance, and then select Wireless Configuration.
     The device discovery process automatically starts.
- **Point Test:**
  1. Start a phone session.
     Refer to *Section 1.3 System Setup* on page 5 for phone session options.
  2. From the Installer Menu:
  - Press [1] to select System Maintenance, and then press [2] to select Full System Test.
    The discovery process starts at the beginning of the Point Test.

    OR
  - Press [1] to select System Maintenance, and then press [3] to select System Test Menu. From the System Test Menu, press [5] to select Point Test.
    The discovery process starts at the beginning of the Point Test.

3.1.2 Establish and Configure the Wireless Network

The wireless hub automatically establishes and configures the wireless network.

The wireless hub evaluates each available radio frequency (RF) for noise, RF signal strength, and other adjacent wireless systems. The wireless hub then selects the frequency with the lowest amount of noise and least amount of traffic for network operation.

To configure the wireless network, the wireless hub selects the best channel for broadcasting. Once a channel is selected, the wireless hub then configures all discovered devices to operate on the selected frequency. This process takes several minutes.

3.1.3 Configure Devices

Input and Output Devices

> The ISW-BMC1-S135X Door/Window Contact and the ISW-BIN1-S135X Inertia Detector have a magnetic switch as an input. If the magnetic switch is not used, remove the magnet from the device before starting the Point Test.

Once the network is established and configured, the system announces "Test all points." Test the wireless devices in this order: input devices, output devices, and relay modules.

> Do not exit the Point Test until all intended wireless devices are tested. Otherwise, you must manually add devices to the system.
>
> If extra wireless devices not intended for installation are within the wireless hub's range, the hub might also discover these devices. To exclude any unused devices from the system, press [#] (or [5] from the control center) to exit the Point Test. The wireless hub returns all unused devices to the undiscovered state.

As you test each device, complete *Section 4.3.5 Point Programming Items* on page 46, and *Section* 4.3.6 Output Programming Items on page 51.

When you restore the device, the system announces the assigned device number.

3.1.4 Test Devices

> Point numbers are assigned to wireless devices in the order that the devices are tested (tampered or faulted and restored). If specific point numbers are preferred for wireless devices, ensure that the wireless devices are tested in the appropriate order. Otherwise, the system assigns the lowest available point number to the first tested wireless device.

Refer to the following table for instructions on testing each wireless device.

Device	To Test:
Motion Detectors	Walk across the detector's coverage pattern.
Smoke Detector	• Press and release the detector's test button, or • Blow smoke into the detector's chamber to cause an alarm. Restore the alarm.
Relay Module	• **Input:** Fault and restore the supervised loop. • **Output:** Tamper the device. Perform both tests only if both the input and output are used.
Inertia Detector	• **Magnetic Switch:** Open and then close the switch. • **Inertia Only:** Cause an alarm and then restore the alarm[1], or tamper the detector.[3]
Glass Break Detector	Cause an alarm and then restore the alarm[2], or tamper the detector.[3]
Mini Door/Window Contact Recessed Door/Window Contact	Open and then close the magnetic switch.
Door/Window Contact	• Open and then close the magnetic switch, or • Fault and then restore the supervised loop. Perform both tests only if both the magnetic switch and supervised loop are used.
Siren	Tamper the device.

[1] To test the inertia detector, create a shock to cause an inertia alarm, and then restore alarm.

[2] To test the glass break detector, use a special tool to cause a glass break alarm, and then restore the alarm.

[3] If you tamper the detector, the control panel enrolls the detector, but does not test it. You must create the appropriate alarm and restore the alarm to test the detector.

Key Fobs

Add key fobs after all other wireless devices (inputs and outputs) are discovered and configured.

1. After the last wireless device is configured and the Point Test ends, press [#] repeatedly until you exit the Installer Menu and end the phone session.
2. Start a new phone session, or press and hold [3] on the control center, and enter the master user (User 1) passcode.
3. Press [4] to select the User Menu.
4. Press [1] to add a new user.
5. Enter a passcode.
6. Re-enter the passcode.
7. Press [4] to add a key fob.
   Token assignment and voice description are optional.
8. Repeat *Steps 4* to *7* to add more users and key fobs, or press [#] repeatedly to end the phone session.

To create a key fob-only system (no wireless input or output devices installed), start at *Step 2*.

In a key fob-only system, adding the first key fob might take several minutes to complete as the wireless network is established and configured. Subsequent key fob additions take less time.

3.2 Wireless Maintenance

3.2.1 Wireless Configuration Menu

Use the Wireless Configuration Menu to:

- Add new wireless devices to an existing wireless system
- Add wireless devices that were not discovered when the wireless network was first discovered
- Replace or delete wireless devices from an existing wireless system

To access the Wireless Configuration menu:

1. Start a phone session.
   Refer to *Section 1.3 System Setup* on page 5 for phone session options.
2. From the Installer Menu, press [1] for System Maintenance.
3. From System Maintenance, press [6] for Wireless Configuration.
   Refer to the following table for menu options and descriptions. Menu options are only available after the initial device discovery and point test is completed.

Button Press	Menu Option	Description
[1]	Replace a Device	Use this option to replace a known device with a new device. 1. Press [1] to replace a point, or [3] to replace an output. For a relay module, select either the input or output, and then enter the appropriate number in *Step 2*. 2. Enter the desired point number or output number. The device discovery process starts. 3. When the system announces "Test all points," activate the new device. The new device replaces the current device. If other devices were discovered in *Step 2*, they are returned to the undiscovered state.
[2]	Add a Device	Use this option to add more devices to the wireless network. When you press [2] to select this option, the device discovery process starts. When the system announces "Test all points," activate all of the new devices. If other devices were discovered but not activated, they are returned to the undiscovered state.
[3]	Delete a Device	Use this option to delete a known device from the system. 1. Press [1] to delete a point, or [3] to delete an output. 2. Enter the desired point number or output number. If the selected point number corresponds with a relay module, **both** the input and output are deleted from the system. If you only want to delete the input or the output, you must disable the corresponding function through programming. 3. Press [1] to delete the device. The wireless hub deletes the device from the system, and the point type or output function is set to 0 (Disabled).
[4]	Transfer Wireless Data (control panel-to-hub)	If you replace a hub, select this option to send wireless data from the control panel to the wireless hub.
[5]	Transfer Wireless Data (hub-to-control panel)	If you replace the control panel, select this option to send wireless data from the wireless hub to the control panel. This option deletes key fobs.
[6]	Erase and Discover	If the wireless data in the control panel does not match the wireless data in the hub (*Bus Device Trouble 50*), use this option to erase the wireless data in both the control panel and hub, and rediscover all devices. This option is only available if the wireless data does not match in the control panel and hub.
[#]	Exit Wireless Configuration	Select this option to return to the System Maintenance options.

3.2.2 Assigning Points 1 to 8 as Wireless Points

To assign an on-board point (1 to 8) as a wireless point, disable the point in programming before starting the device discovery process.

You can individually assign Points 1 to 8 as wireless points.

3.2.3 DX2010 Input Expanders and Wireless Points

If Points 9 to 32 contain wired and wireless points, install all required DX2010 Input Expanders **before** adding any wireless points to the system.

Adding a DX2010 Before Adding Wireless Points

The control panel supports up to three DX2010 modules. Each module occupies a group of eight points.

The DX2010's DIP switch address determines which group of points the DX2010 occupies:

- **Address 102:** DX2010 occupies Points 9 to 16
- **Address 103:** DX2010 occupies Points 17 to 24
- **Address 104:** DX2010 occupies Points 25 to 32

Refer to *Section 2.4 DX2010 Installation* on page 12 for more DIP switch settings.

As each DX2010 module is added to the system, it occupies the next available group of points.

For Points 9 to 32, wireless points also occupy points in the same groups of eight as the DX2010 modules:

- If you add a DX2010 module using Address 102 (Points 9 to 16), wireless points can only occupy Points 17 to 32.
- If you add two DX2010 modules using Addresses 102 (Points 9 to 16) and 103 (Points 17 to 24), wireless points can only occupy Points 25 to 32.
- If you add three DX2010 modules, wireless points can only occupy Points 1 to 8.

Adding a DX2010 After Adding Wireless Points

If you add a DX2010 module after wireless points are added, based on its DIP switch address, the DX2010 replaces the conflicting group of wireless points.

For example, if wireless points occupy Points 9 to 24, and you need Points 17 to 24 as wired points, a DX2010 module with Address 103 replaces the wired points occupying Points 17 to 24.

If the next point grouping is available, for this example, Points 25 to 32, the control panel retains all point programming except for voice descriptions, and moves the conflicting wireless points to the next point grouping. You must re-record voice descriptions for the points that were moved.

If the next point grouping is **not** available, the control panel deletes the conflicting wireless points from the system.

3.2.4 Recovering the Wireless Network

Expert Programming Item Number 9999 restores the control panel to its factory default settings. All wireless network data in the control panel is lost, but is retained in the wireless hub.

To recover wireless network data from the wireless hub:

1. Start a phone session.
2. Press [1] to select System Maintenance.
3. Press [6] to select the Wireless Configuration Menu.
4. Press [5] to transfer wireless data from the hub to the control panel.
   This option deletes key fob assignments. You must reassign all key fobs.

3.3 Wireless System Messages

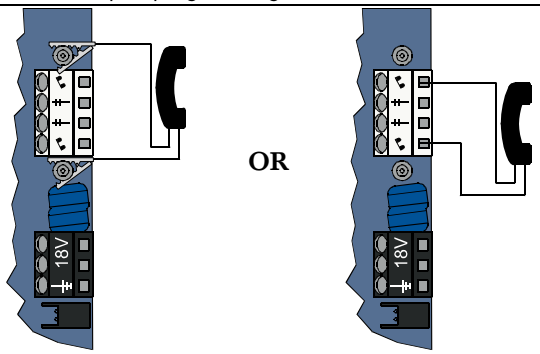
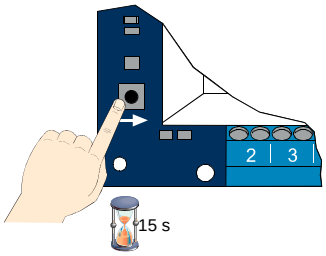
Refer to the following table for a description of system messages that pertain to the wireless network.

System Message	Description
"Wireless devices not configured."	Point Test was exited before all wireless points were tested.
"Extra device ignored."	An attempt was made to add a device to a system that already contains the maximum number of points or outputs.
"Point x was tested."	A point was tested. RFSS is acceptable.
"Point x low."	A point was tested. RFSS is unacceptable.
"Please wait."	The wireless network is busy, or the control panel is waiting for the wireless network to respond. The control center might show a single rotating segment of the circle of protection with this message.
"Wireless error."	The wireless hub is jammed, missing, or experiencing a trouble condition.
"Wireless devices x."	"x" = the number of devices that are discovered, but not tested.
"Wireless devices not tested x."	"x" = the number of devices that are discovered, but not yet configured.
"Point x not tested."	The control panel assigned a point number to the device, but the device was not tested (faulted, or tampered, and restored). "x" = the voice description. By default, the system announces the point number.

4.0 Programming

4.1 Enter Programming

Select one of the following methods to enter the Installer Menu:

Method	Steps
House Phone	1. Press [#][#][#]. 2. Listen for the voice prompt to enter a passcode. 3. Enter the installer passcode.[1] 4. Press [3] for basic programming, or [4] for expert programming.
Outside Phone	1. Call the premises phone number. 2. After the call is answered by either a person or a telephone answering device, press [*][*][*] to disconnect the answering party and access the system. If the phone is not answered by a person or telephone answering device, the system answers after a programmed number of rings. Refer to *Expert Programming Item Number 222* on page 42. 3. Listen for the voice prompt to enter a passcode. 4. Enter the installer passcode.[1] 5. Press [3] for basic programming, or [4] for expert programming.
Installer Quick Connect[2]	1. Connect a phone set to either the test posts or the phone terminals.  2. Press and hold the System Test button for approximately 15 sec.  3. Listen for the voice prompt to enter a passcode. 4. Enter the installer passcode.[1] 5. Press [3] for basic programming, or [4] for expert programming.
RPS	Refer to *Section 4.6 Remote Programming Software (RPS)* on page 55 for more information.

[1] If the passcode length = four digits, the default installer passcode is 5432. If the passcode length = six digits, the default installer passcode is 543211. Refer to *Section 4.3.8 User Programming Items* on page 53 to change the passcode length and the installer passcode.

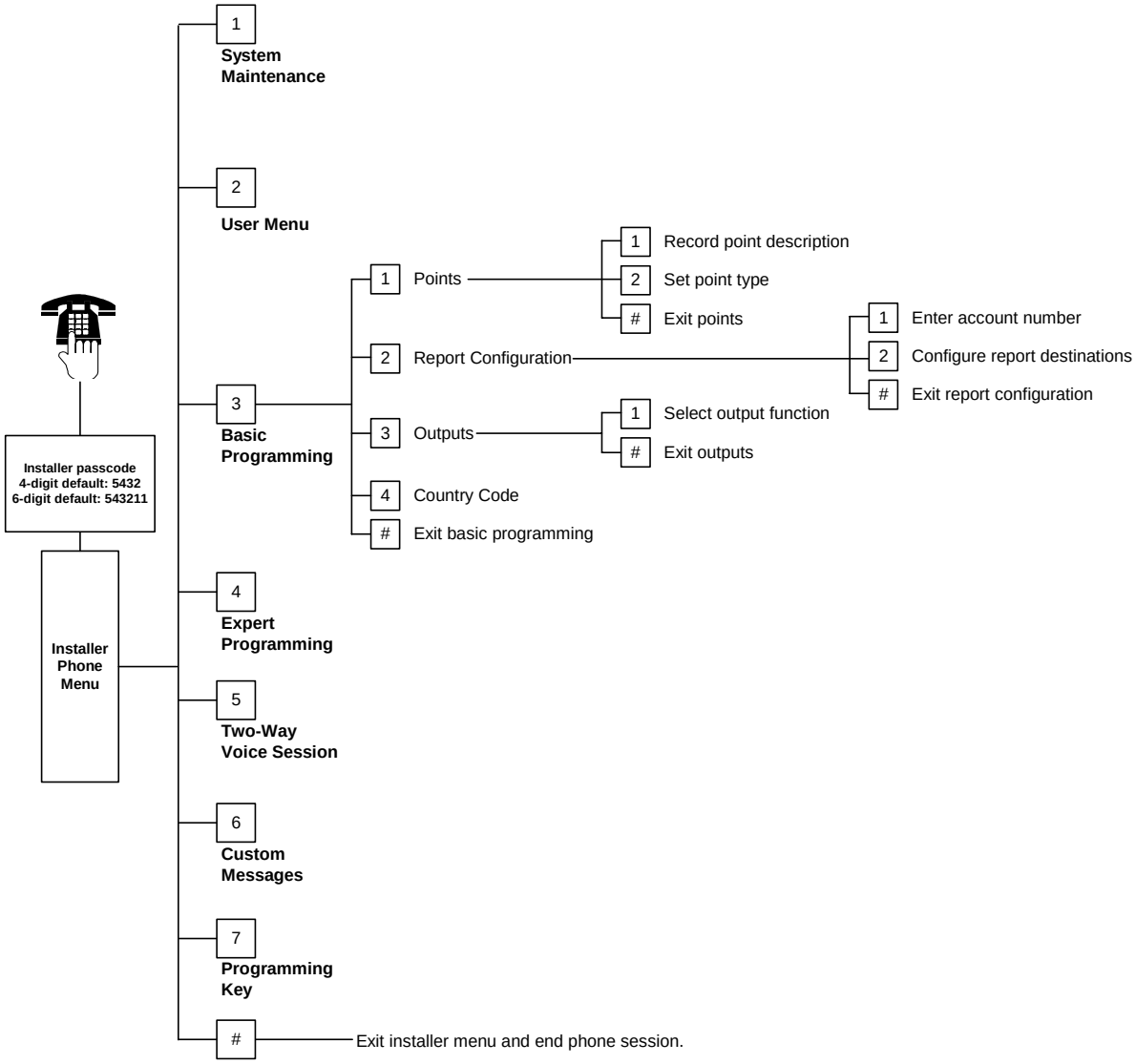
[2] Select the installer quick connect method if a phone line is not available, or a local connection is required. The system must be off to use this method.

First Time Programming

1. Set the country code to the appropriate code for your installation before making any other programming changes.
   This selection sets control panel's defaults to the appropriate country-specific values. Refer to *Section 4.2.4 Country Code* on page 34.
2. Set the time and date. Refer to *Section 1.5 Installer Phone Menu* on page 6.

4.2 Basic Programming

Basic programming consists of a voice menu that contains the essential programming items. Generally, finishing this programming section is usually all that is required for a complete system



4.2.1 Points

You cannot program any wireless points without first completing the steps in *Section 1.4 System Setup* on page 5.

Points Enter a point number from 1 to 32.

1 **Record Point Description**

For example, if Point 1 is located at the building's front door, say "Front Door" at the tone.

Press [1] to continue programming the selected point.

Press [2] to re-record your current point description.

2 **Set Point Type**

Press [1] to select the current option.

Press [2] to hear more options.

Press [#] to exit Point Type.

Point Type	Description
Disabled	Point is disabled.
Perimeter (Entry or Exit)*	If faulted and the system is on, Entry Delay starts. An alarm occurs if the system is not turned off when Entry Delay ends.
Interior (Follower)*	If the system is on occupied, it ignores these points. If the system is on unoccupied, a faulted interior point starts an alarm. These points are ignored during Exit and Entry Delay times.
Perimeter Instant*	If faulted when the system is on, a local alarm occurs.
24-Hour	If faulted, an alarm always occurs. To restore a 24-hour point, turn the system off if it is on, or acknowledge the alarm if the system is off.
Fire Verified	If faulted, fire verification occurs. If a second fire event occurs during the two-min. wait period, a fire alarm occurs. If no second fire event occurs, the system returns to normal.
Fire Instant	If faulted, a fire alarm always occurs.
Silent Panic	If faulted, an alarm always occurs. There is no visual or audio indication of the alarm.
Interior Walkthrough*	If faulted and the system is on custom protection, Entry Delay starts. If the system is on occupied or unoccupied, this point functions as an interior point.
Perimeter Exit Cancel*	If faulted and restored during Exit Delay, Exit Delay stops and the system immediately turns on.
Momentary Keyswitch	Turn the system on or off using a momentary keyswitch.
Maintained Keyswitch	Turn the system on or off using a maintained keyswitch.

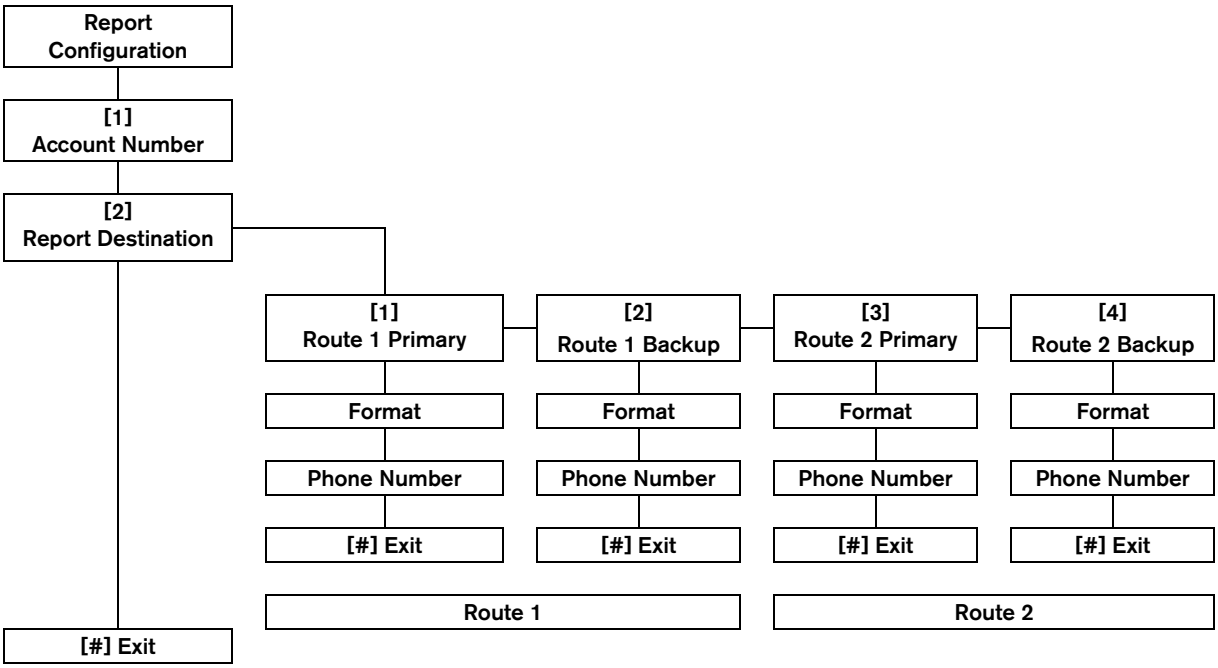
**Exit Points**

Return to the Installer Menu.

* An alarm report is not sent to the central station if the system is turned off within the abort window.

Record point programming entries in the *Point Programming Entry Tables* starting on page 47.

4.2.2 Report Configuration



To configure reports:

1. Enter a four- or six-digit account number. The account number applies to all report destinations.
2. Select a report destination.
   [1] = Route 1 Primary
   [2] = Route 1 Backup
   [3] = Route 2 Primary
   [4] = Route 2 Backup
3. Select a format option for the report destination.
   [1] = Select first option.
   [2] = Hear next option.
4. Enter a phone number for the report destination.
5. Repeat *Steps 2* to *4* for additional report destinations.
6. Refer to *Section 4.3.4 Report Routing Programming Items* on page 43 to enable or disable reports.

Account Number Entries:

Entry	Key Press
0 to 9	[0] to [9]
B	[*][1]
C	[*][2]
D	[*][3]
E	[*][4]
F	[*][5]

Phone Number Entries:

Entry	Key Press
0 to 9	[0] to [9]
*	[*][*]
#	[*][#]
Pause	[*][1]
Exit with Save	[#]
Exit without Save	[#][#][1]
Disable phone number	[0][#]

[1] Press [#] twice within two seconds to exit without saving your entry.

Format Options:

- Disabled (default)
- Contact ID
- SIA
- Voice
- SMS Text (TAP)*
- Fast Format

* SMS Text Messages:

- Intrusion Alarm
- Fire Alarm
- System On
- System Off
- Point Trouble
- System Trouble
- Test Report
- Restoral
- Keypad

SMS providers do not guarantee delivery of SMS text messages.

Record report configuration programming entries in *Section 4.3.3 Communicator Programming Items* on page 41.

4.2.3 Outputs

You cannot program any wireless outputs without first completing the steps in *Section 1.4 System Setup* on page 5

Output devices consist of horns, bells, or strobes.

Outputs Enter an output number from 1 to 8.

1 **Output Function**

Press [1] to select the current option.

Press [2] to hear more options.

Press [#] to exit Output Function.

Output Function	Description
Disabled	Output is disabled.
Intrusion	Output turns on when intrusion alarm occurs. To turn off output, turn off system, or wait until end of intrusion bell cut-off time.
Intrusion Latching	Output turns on when intrusion alarm occurs. To turn off output, turn off system.
Fire	Output turns on when a fire alarm occurs. To turn off output, turn off system if it is already on, or wait until end of fire bell cut-off time.
Fire Latching	Output turns on when a fire alarm occurs. To turn off output, turn off system if it is already on, or acknowledge alarm if system is off.
Intrusion and Fire	Output turns on when an intrusion or fire alarm occurs. To turn off output, turn off system, or wait until end of bell cut-off time. Fire alarms take priority over intrusion alarms.
Intrusion and Fire Latching	Output turns on when an intrusion or fire alarm occurs. To turn off output, turn off system if it is already on, or acknowledge alarm if system is off. Fire alarms take priority over intrusion alarms.
System Reset	Output is normally on. Output turns off for approximately 10 sec when system is reset. Use this function to supply power to devices such as four-wire smoke detectors that require power interruption to reset a latching alarm condition.
System On	Output turns on when the system is turned on, and remains on until system is turned off.
System Ready	Output turns on when the system is ready to turn on (no faulted points or system troubles exist).
Key Fob On/Off	Output turns on or off when the user presses the key fob's  or  key. Refer to *Expert Programming Item Numbers 616* and *626* on page 40 for more information.
Key Fob 2-sec Pulse	Output turns on for two seconds when the user presses the key fob's  or  key. Refer to *Expert Programming Item Numbers 616* and *626* on page 40 for more information.
User Controlled	Output turns on or off when a user or the installer uses the Operate Outputs option from the phone menus.

**Exit Outputs**

Return to the Installer Menu.

Record output programming entries in *Section* 4.3.6 *Output Programming Items* on page 51.

4.2.4 Country Code

Select the appropriate country code for your installation. This code sets the control panel to the appropriate country-specific defaults.

A

Country	Code
Afghanistan	65
Albania	65
Algeria	63
American Samoa	65
Andorra	65
Angola	65
Antigua	65
Argentina	01
Armenia	62
Australia	02
Austria	03
Azerbaijan	65

B

Country	Code
Bahamas	65
Bahrain	63
Bangladesh	65
Barbados	65
Barbuda	65
Belarus	62
Belgium	04
Belize	65
Benin	65
Bhutan	65
Bolivia	65
Bosnia	65
Botswana	65
Brazil	05
Brunei	65
Bulgaria	06
Burkina Faso	65
Burma (Myanmar)	65
Burundi	65

C

Country	Code
Cambodia	65
Cameroon	65
Canada	07
Cape Verde	65
Central African Republic	65
Chad	65
Chile	65
China	08
Colombia	09
Comoros	65
Congo (Brazzaville)	65
Congo (Kinshasa)	65
Costa Rica	65
Croatia	10
Cuba	65
Cyprus	11
Czech Republic	12

D

Country	Code
Denmark	13
Dijibouti	65
Dominica	65
Dominican Republic	65

E

Country	Code
East Timor	65
Ecuador	65
Egypt	14
El Salvador	65
Equatorial Guinea	65
Eritrea	65
Estonia	15
Ethiopia	65

F

Country	Code
Fiji	65
Finland	16
France	17
French Polynesia	63

G

Country	Code
Gabon	65
Gambia	65
Georgia	62
Germany	18
Ghana	65
Greece	19
Greenland	65
Grenada	65
Grenadines	65
Guatemala	65
Guinea	65
Guinea-Bissau	65

H

Country	Code
Haiti	65
Herzegovina	65
Holy See	65
Honduras	65
Hong Kong	20
Hungary	21

I

Country	Code
Iceland	63
India	22
Indonesia	23
Iran	65
Iraq	65
Ireland	24
Israel	63
Italy	25
Ivory Coast	65

J

Country	Code
Jamaica	65
Japan	26
Jordan	62

K

Country	Code
Kazakstan	62
Kenya	65
Kiribati	65
Korea, North	65
Korea, South	27
Kuwait	65
Kyrgystan	62

L

Country	Code
Laos	65
Latvia	28
Lebanon	63
Lesotho	65
Liberia	65
Libya	65
Liechtenstein	63
Lithuania	29
Luxembourg	30

M

Country	Code
Macedonia	31
Madagascar	65
Malawi	65
Malaysia	32
Maldives	65
Mali	65
Malta	33
Marshall Islands	65
Mauritania	65
Mauritius	65
Mexico	34
Micronesia	65
Moldova	62
Monaco	65
Mongolia	65
Morocco	63
Mozambique	65

N

Country	Code
Namibia	65
Nauru	65
Nepal	65
Netherlands	35
Nevis	65
New Zealand	36
Nicaragua	65
Niger	65
Nigeria	37
Norway	38

O

Country	Code
Oman	62

P

Country	Code
Pakistan	62
Palau	65
Panama	65
Papua New Guinea	65
Paraguay	65
Peru	39
Philippines	40
Poland	41
Portugal	42
Principe	65

Q

Country	Code
Qatar	62

R

Country	Code
Romania	43
Russian Federation	44
Rwanda	65

S

Country	Code
St. Kitts	65
St. Lucia	65
St. Vincent	65
San Marion	65
Sao Tome	65
Saudi Arabia	45
Senegal	65
Serbia	46
Seychelles	65
Sierra Leone	65
Singapore	47
Slovakia	48
Slovenia	49
Soloman Islands	65
South Africa	50
Spain	51
Sri Lanka	65
Sudan	65
Suriname	65
Swazilands	65
Sweden	52
Switzerland	53
Syria	62

T

Country	Code
Taiwan	54
Tajikistan	65
Tanzania	65
Thailand	55
Togo	65
Tonga	65
Trinidad and Tobago	65
Tunisia	65
Turkey	56
Turkmenistan	65
Tuvalu	65

U

Country	Code
Uganda	65
Ukraine	62
United Arab Emirates	65
United Kingdom	57
United States	58
Uruguay	65
Uzbekistan	65

V

Country	Code
Vanuatu	65
Venezuela	59
Vietnam	60

Y

Country	Code
Yemen	65

Z

Country	Code
Zambia	63
Zimbabwe	65

4.3 Expert Programming

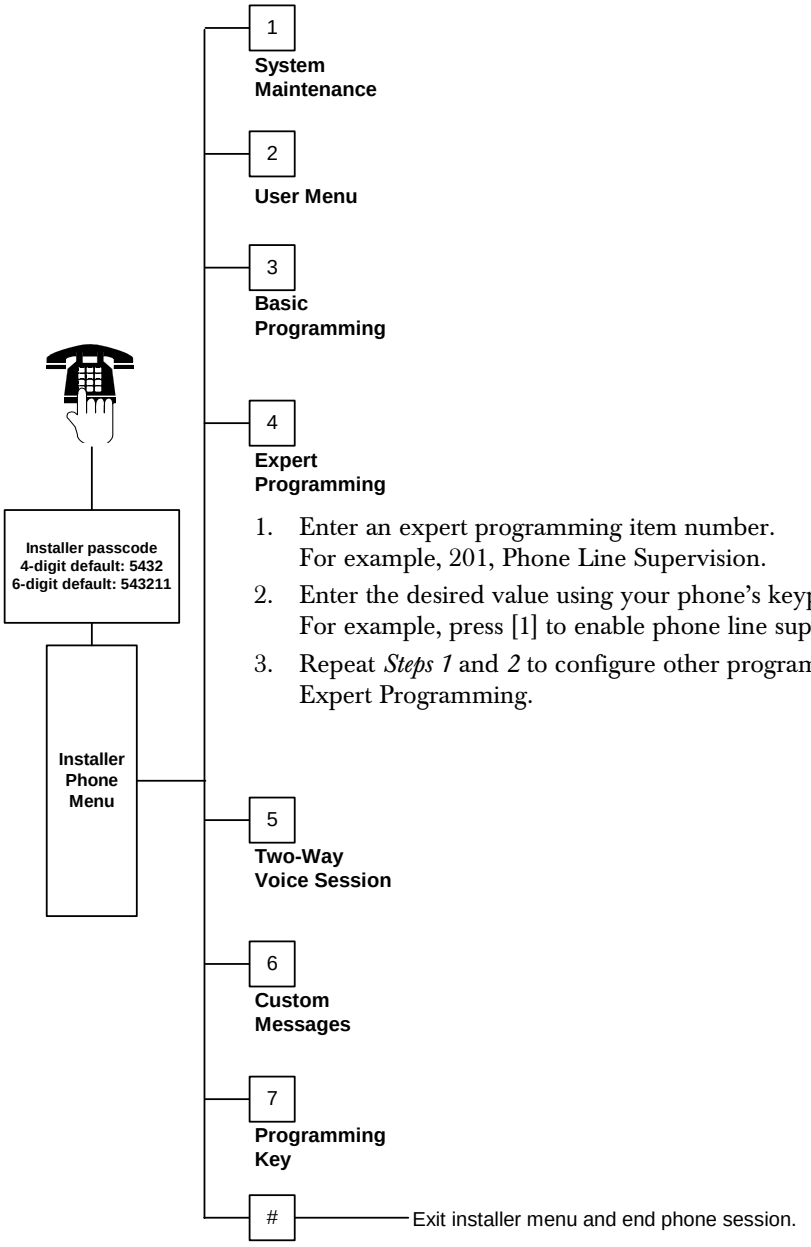
Only use expert programming if you have a special programming requirement.

To comply with specific agency requirements, refer to *Section 7.7 Agency Approvals and Requirements* on page 68 for any necessary programming changes.

Expert programming allows access to all programming categories for full system configuration:

- System
- Communicator
- Report routing
- Points
- Outputs
- Control centers
- Users

Each category consists of several related programming items. Each programming item is assigned a three- or four-digit number.



1. Enter an expert programming item number.
   For example, 201, Phone Line Supervision.
2. Enter the desired value using your phone's keypad.
   For example, press [1] to enable phone line supervision.
3. Repeat *Steps 1* and *2* to configure other programming items, or press [#] to exit Expert Programming.

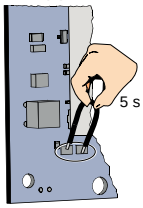
4.3.1 ROM Firmware Version Items

Programming Item	Item Number	Description
Control Panel Firmware Version	090	System announces the installed firmware version. This item is read-only.
Control Center 1 Firmware Version	091	System announces the installed firmware version for the selected control center. These items are read-only.
Control Center 2 Firmware Version	092	
Control Center 3 Firmware Version	093	
Control Center 4 Firmware Version	094	

4.3.2 System Programming Items

Programming Item	Item Number	Description (Range)	Entry
Country Code	102	Select the appropriate code for country-specific operation and programming defaults (00 to 65).	58
Enclosure Tamper Enabled	103	0 = Enclosure tamper input disabled 1 = Enclosure tamper input enabled	1
Fire Bell Cut-Off Time	107	Enter how long the fire alarm sounds at bell outputs and at the control center (0 to 90 min).	5
Intrusion Bell-Cut off Time	108	Enter how long the intrusion alarm sounds at bell outputs and at the control center (0 to 90 min).	5
Intrusion Abort Window	110	Enter how long the control panel waits to send an alarm report after an alarm occurs (15 to 45 sec).	30
Intrusion Cancel Window	112	Enter how long a user has to cancel an intrusion alarm report after the system sends the report to the central station (5 to 10 min).	5
Chime Tone Select	114	Select a Chime tone: 1 = Chime door bell 2 = Single chime 3 = Standard door bell	1
Chime Mode Operation After System Off	115	Determines Chime Mode operation after the system is turned off. 0 = Off 1 = On 2 = Follows previous setting (either on or off)	0
Automatic Test Report Frequency	116	Determines how often the control panel sends the automatic test report. 0 = No automatic test report 1 = Daily (refer to *Programming Items 143* and *144* on page 40) 2 = Weekly (refer to *Programming Item 145* on page 40) 3 = Monthly (refer *to Programming Item 146* on page 40)	0
RPS Passcode	118	Enter the 6-digit passcode that allows access to the control panel from RPS. Use digits 0 to 9 and A to F.	123456
Daylight Saving Time Operation	121	0 = No time adjustment 1 = North America (prior to 2007) 2 = Europe and Asia 3 = Tasmania, Australia 4 = Rest of Australia 5 = New Zealand 6 = Cuba 7 = South America and Antarctica 8 = Namibia, Africa 9 = USA after 2006	1

Default = Country-specific default. Select this programming item to hear the updated default value.

Programming Item	Item Number	Description (Range)	Entry
Installer Passcode Override Enabled	122	0 = Override disabled 1 = Override enabled To override the installer passcode prompt, short solder pads together for approximately 5 sec (see below).  Pick up phone to hear Installer Menu options.	1
Programming Key Auto Transfer	123	0 = Installer must activate the programming key from the Installer Menu. 1 = Programming key automatically sends or receives stored programming data. Refer to *Section 4.5 Programming Key* on page 54 for more information.	1
Point Alarm Verification	124	Determines the level of alarm verification required by point before generating an intrusion alarm condition. 0 = None Point generates an alarm as soon as the condition is detected. 1 = Cross zone To cause an alarm, two or more Cross Zone points must be faulted within the time set in *Expert Programming Item Number 134* (refer to page 39). Cross Zone Enabled must = 1 for at least two interior or perimeter points. Refer to *Section 4.3.5 Point Programming Items* on page 46. 2 = Intelligent threat assessment Protection levels, point types and conditions, and system event timing are used to assess a potential threat. If the threat reaches a specific threshold, the system sends a verified alarm report. 3 = Confirmed alarms Opening the initial entry door disables all means of alarm confirmation. 4 = Confirmed alarms Use a token, key fob, or key from a keyswitch to turn the system off.	0
Faulted Points Allowed Threshold	125	Determines the maximum number of faulted points that are disabled while the system is on (0 to 8).	3
Exit Delay	126	Enter how long the user has to exit the building before the system turns on (45 to 255 sec).	60
Entry Delay	127	Enter how long the user has to enter the building and turn off the system before an alarm condition occurs (30 to 255 sec).	30
Exit Time Restart	128	0 = User cannot reset Exit Delay timer. 1 = User can reset Exit Delay timer once while system is on. If the system is in Exit Delay, and a Perimeter point faults, restores, and faults again, the Exit Delay timer resets.	1
Recent Close Enabled	129	0 = Recent Close report not sent. 1 = Recent Close report sent within two min of turning on the system.	1

Default = Country-specific default. Select this programming item to hear the updated default value.

Programming Item	Item Number	Description (Range)	Entry
Swinger Bypass Count	131	1 = One alarm report allowed from point while system is on before point is bypassed. 2 = Two alarm reports allowed from point while system is on before point is bypassed. 3 = Three alarm reports allowed from point while system is on before point is bypassed.	1
Auto Protection Level	132	0 = System always turns on (unoccupied) when selected. 1 = System only turns on (unoccupied) if a perimeter point is faulted during Exit Delay. If no point is faulted, the system turns on (occupied).	1
System On Order Options	133	Determines the order that system-on options are announced to the user. 1 = "Stay[1]," "Leave[2]," "Custom[3]" 2 = "Stay," "Custom," "Leave" 3 = "Leave," "Stay," "Custom" 4 = "Leave," "Custom," "Stay" 5 = "Custom," "Leave," "Stay" 6 = "Custom," "Stay," "Leave" [1] "Stay" = System On Occupied [2] "Leave" = System On Unoccupied [3] "Custom": Only announced if points are programmed as Custom Protection points. Refer to Section *4.2.1 Point Programming Items* on page 46 to assign Custom Protection points.	1
Cross Zone Timer	134	Enter how long the system waits for at least two Cross Zone points to be faulted before the control panel sends a Verified Alarm report to the central station (60 to 3600 sec). If only one Cross Zone point is faulted during this time, the control panel sends an Unverified Alarm report to the central station. The cross zone timer is also used as the confirmed alarm timer.	120
Restricted Alarm Memory	136	0 = Any user can clear the alarm memory. 1 = Only the master user can clear the alarm memory.	0
Latching Point and Enclosure Tamper	137	0 = Any user token or passcode can clear a point or enclosure tamper condition. 1 = Only the installer passcode can clear a point or enclosure tamper condition.	0
Latching System Device Tamper	138	0 = Any user token or passcode can clear a tamper condition from a system device (control center, DX2010, or wireless hub). 1 = Only the installer passcode can clear a tamper condition from a system device.	0
Verbose System Test Enabled	139	0 = Internal tests are conducted silently, and the control center announces the entire test status when all tests are complete. 1 = The control center announces tests as they are performed.	1
Demo Mode	140	0 = The system only announces all telephone menu messages over the phone. 1 = The system announces all telephone menu messages over the phone and at all control centers connected to the system.	0
Restrict Installer Passcode	142	0 = Master user passcode or token not needed to enable Installer Passcode. 1 = Master user must present token or enter passcode before installer enters Installer Passcode. Installer passcode is enabled until a user turns the system on. The master user can also enable installer access from the User Phone Menu ([3] System Maintenance → [6] Expert Programming). Refer to page 7 for more information. This setting also restricts the availability of certain Installer Menu options.	0

Default = Country-specific default. Select this programming item to hear the updated default value.

Programming Item	Item Number	Description (Range)	Entry
Test Report Hour	143	Enter the hour that the control panel sends the test report (0 to 23).	8
Test Report Minute	144	Enter the minute that the control panel sends the test report (0 to 59).	0
Test Report Day of Week	145	Select the day that the control panel sends the test report. *Program Item 116* must = 2 (Weekly). 0 = Sunday 1 = Monday 2 = Tuesday 3 = Wednesday 4 = Thursday 5 = Friday 6 = Saturday	0
Test Report Day of Month	146	Enter the day of the month that the control panel sends the test report (1 to 28). *Expert Programming Item Number 116* must = 3 (Monthly).	1
Restrict Confirmed Alarm Memory	147	0 = User passcode can clear a confirmed alarm. 1 = Only installer passcode can clear a confirmed alarm.	0
Arming Beeps/Graduated Annunciation	148	0 = No arming beeps from control center and no outputs activation during Entry Delay. 1 = No arming beeps from control center, but outputs activate during Entry Delay. 2 = Control center sounds arming beeps, but outputs do not activate during Exit Delay. 3 = Control center sounds arming beeps and outputs activate during Entry Delay.	0
Wireless Jam Detect Level	150	Configure the jam detect level of the wireless devices (0 to 15).	12
Key Fob Arming	153	0 = Do not turn system on if there are faulted points 1 = Force arm faulted points if the number of faulted points is within the range set in *Expert Programming Item Number 125* (refer to page 38) 2 = Force arm faulted points even if the number of faulted points exceeds the range set in *Expert Programming Item Number 125*	0
Two-Way Voice Session Configuration	158	0 = Allow two-way voice session to occur at any time 1 = Restrict two-way voice session to occur only during alarm conditions	0
Start Arming with Faulted Points	159	0 = All faulted points must be force armed before the system can be turned on 1 = Exit Delay starts with faulted points	1
Speak Active Faults	160	0 = Control center only speaks “Call for Service” when a fault occurs 1 = Control center speaks fault condition	0
Wireless Transmission Attenuation	161	0 = No signal attenuation 1 = 3 dB attenuation for EN 50131 Security Grade 1 2 = 6 dB attenuation for EN 50131 Security Grade 2 3 = 9 dB attenuation for EN 50131 Security Grade 3 4 = 12 dB attenuation for EN 50131 Security Grade 4	0
Key Fob Button Configuration 	616	0 = Status request only 1 = Turn system on (occupied) 2 = Turn system on (custom protection) 3 = Turn output on or off 4 = Turn output on for 2 sec.	0
Key Fob Button Configuration 	626	0 = Status request only 1 = Turn system on (occupied) 2 = Turn system on (custom protection) 3 = Turn output on or off 4 = Turn output on for 2 sec.	0

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.3 Communicator Programming Items

To enable reporting, configure the following programming items:

- Account Number (*Expert Programming Item Number 100*)
- Route 1 Primary Destination (*Expert Programming Item Number 206*)
- Route 1 Backup Destination (*Expert Programming Item Number 207*) – optional
- Route 2 Primary Destination (*Expert Programming Item Number 208*) – optional
- Route 2 Backup Destination (*Expert Programming Item Number 209*) – optional
- Format for Route 1 Primary Destination (*Expert Programming Item Number 211*)
- Format for Route 1 Backup Destination (*Expert Programming Item Number 212*) – optional
- Format for Route 2 Primary Destination (*Expert Programming Item Number 213*) – optional
- Format for Route 2 Backup Destination (*Expert Programming Item Number 214*) – optional

To enable or disable reports, refer to *Section 4.3.4 Report Routing Programming Items* on page 43.

Programming Item	Item Number	Description (Range)	Entry
Account Number	100	Enter a 4- or 6-digit account number (0000 to FFFFFF). Valid digits are 0 to 9 and B to F. Do not use "A."	000000
Phone Line Supervision	201	0 = Phone line is not supervised. 1 = Phone line is supervised.	0
Voice Format Repeat Count	203	Enter the number of times the system repeats a voice report during the phone call (1 to 15).	3
Voice Format Message Delivery Attempts	204	Enter how many times the system attempts to deliver a voice format message (1 to 5). The time delay between delivery attempts increases by 5 sec.	1
Dial Tone Detect	205	0 = Do not wait for dial tone before dialing central station. 1 = Wait for dial tone before dialing central station.	1
Route 1 Primary Destination	206	Enter a phone number for each destination (up to 32 digits): 0 to 9 = [0] to [9] * = [*][*] # = [*][#] Pause = [*][1] Exit with save = [#] Exit without save = [#][#] Press [#] twice within two seconds to exit without saving your entry. Disable phone number = [0][#]	0
Route 1 Backup Destination	207		0
Route 2 Primary Destination	208		0
Route 2 Backup Destination	209		0
SMS Service Provider Number	210	Enter your cellular phone service provider's phone number for text messaging (up to 32 digits). For SMS providers that support TAP protocol, contact your cellular provider, or visit www.notepager.com/tap-phone-numbers.htm	0
Format for Route 1 Primary Destination	211	0 = Disabled 1 = Contact ID 2 = SIA 3 = Voice 4 = SMS Text (TAP)* 5 = Fast Format * Refer to page 32 for SMS text messages. SMS providers do not guarantee delivery of SMS text messages.	0
Format for Route 1 Backup Destination	212		0
Format for Route 2 Primary Destination	213		0
Format for Route 2 Backup Destination	214		0

Default = Country-specific default. Select this programming item to hear the updated default value.

Programming Item	Item Number	Description (Range)	Entry
Call Waiting Disable	215	Enter a 3-digit string. Dial this first before dialing the premises phone number. * = [*][*]; # = [*][#] Dialing a call waiting sequence on a non-call waiting phone line prevents the system from successfully contacting the central station.	0
Emergency Call Override Number	216	Enter a 3-digit emergency number, such as 911. If a user dials this number, the system waits the amount of time entered in *Expert Programming Item Number 217* before sending reports.	000
Emergency Call Override Number Delay	217	Enter the amount of time the system waits before sending reports if an emergency number is dialed (0 to 60 min).	5
Auto Detect Pulse Dial	218	0 = Tone dialing only 1 = Auto Detect Pulse or Tone	0
Phone Answer Ring Count	222	Enter the number of rings before the system answers an incoming call (1 to 255 rings).	10
Bell Test	223	This programming item applies to all Intrusion output types and to all arming modes. 0 = No closing ring-back or bell test 1 = Enabled If closing reports are disabled, the outputs turn on for 1 sec at the end of Exit Delay. If closing reports are enabled, the outputs turn on for 1 sec. when the control panel receives a closing report acknowledgement from the central station.	0

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.4 Report Routing Programming Items

Point Report and Restoral Routing

Programming Item	Item Number	Description	Entry
Point Reports and Restorals (all)	**301**	Enter a value in *Expert Programming Item Number 301* to globally set all of the following Point reports and Point Restoral reports to the same entry.	3
Intrusion Alarm	307	To modify only a specific report, enter a value in that report's item number. 0 = Neither route 1 = Route 1 only Primary and Backup (if programmed) 2 = Route 2 only Primary and Backup (if programmed) 3 = Both routes Primary and Backup (if programmed)	3
Intrusion Alarm Verified	308		3
Intrusion Alarm Unverified	309		3
Intrusion Alarm 24-hr	310		3
Intrusion Alarm 24-hr Restoral	311		3
Intrusion Alarm Restoral	312		3
Duress	313		3
Fire Alarm	315		3
Fire Alarm Unverified	316		3
Fire Alarm Restoral	317		3
Panic	318		3
Cancel	323		3
Intrusion Trouble	324		3
Intrusion Trouble Restoral	325		3
Intrusion Zone Bypass	326		3
Intrusion Zone Bypass Restoral	327		3
Fire Trouble	328		3
Fire Trouble Restoral	329		3
Point Missing	333		3
Point Missing Restoral	334		3
Wireless Point Tamper	335		3
Wireless Point Tamper Restoral	336		3
Wireless Point Low Battery	360		3
Wireless Point Low Battery Restoral	361		3
Point Tamper	388		3
Cross Zone Trouble	393		3
Alarm Recent Close	394		3
Panic Restoral	399		3
Cross Zone Trouble Restoral	400		3
Swinger Shunt Bypass	401		3
Swinger Shunt Restoral	402		3

System On and Off Report Routing

Programming Item	Item Number	Description	Entry
System On and Off (open and close) Reports (all)	**302**	Enter a value in *Expert Programming Item Number 302* to globally set all of the following Point reports and Point Restoral reports to the same entry.	3
Exit Error	314	To modify only a specific report, enter a value in that report's item number. 0 = Neither route 1 = Route 1 only Primary and Backup (if programmed) 2 = Route 2 only Primary and Backup (if programmed) 3 = Both routes Primary and Backup (if programmed)	3
Recent Closing	330		3
Close (System On) Unoccupied	337		3
Close (System On) Occupied	338		3
Close Keyswitch	339		3
Close Remote	340		3
Open	341		3
Open Keyswitch	342		3
Open Remote	343		3
Close (System On) Custom	344		3
Partial Close (System On)	403		3

System Report and Restoral Routing

Programming Item	Item Number	Description	Entry
System Reports and Restorals (all)	**303**	Enter a value in *Expert Programming Item Number 303* to globally set all of the following Point reports and Point Restoral reports to the same entry.	3
User Emergency*	319	To modify only a specific report, enter a value in that report's item number. 0 = Neither route 1 = Route 1 only Primary and Backup (if programmed) 2 = Route 2 only Primary and Backup (if programmed) 3 = Both routes Primary and Backup (if programmed)	3
User Fire*	320		3
User Fire Restoral	321		3
User Panic*	322		3
AC Fail	345		3
AC Fail Restoral	346		3
Auto System Test Normal	347		3
Auto System Test Off-Normal	348		3
Auxiliary Power Fault	349		3
Auxiliary Power Restoral	350		3
Communication Fail	351		3
Communication Restoral	352		3
Control Center Supervision Fail	353		3
Control Center Supervision Restoral	354		3
Control Center Tamper	355		3
Control Center Tamper Restoral	356		3

* To enable the control center's emergency buttons, ensure that the following programming items are set accordingly:

Programming Item	Item Number	Setting
User Emergency	319	1, 2, or 3 (refer above for descriptions)
Medical Button Alarm	889	1 (refer to *Global Control Center Items* on page 52 for descriptions)
User Fire	320	1, 2, or 3 (refer above for descriptions)
Fire Button Alarm	888	1 (refer to *Global Control Center Items* on page 52 for descriptions)
User Panic	322	1, 2, or 3 (refer above for descriptions)
Panic Button Alarm	890	1 or 2 (refer to *Global Control Center Items* on page 52 for descriptions)

Check the appropriate box in the *Easy Series User Guide* (P/N: F01U025111) to identify which buttons are enabled.

System Report and Restoral Routing (continued)

Programming Item	Item Number	Description	Entry
Local Programming Success	357	To modify only a specific report, enter a value in that report's item number. 0 = Neither route 1 = Route 1 only Primary and Backup (if programmed) 2 = Route 2 only Primary and Backup (if programmed) 3 = Both routes Primary and Backup (if programmed)	3
Low Battery	358		3
Low Battery Restoral	359		3
Communication Test Manual	362		3
Phone Line Fault	363		3
Phone Line Fault Restoral	364		3
Remote Programming Failure	365		3
Remote Programming Success	366		3
Wireless Receiver Jammed	367		3
Wireless Receiver Jammed Restoral	368		3
Bus Device Tamper	369		3
Bus Device Tamper Restoral	370		3
Bus Device Trouble	373		3
Bus Device Trouble Restoral	374		3
ROM Fault	375		3
Bell Trouble	376		3
Bell Restoral	377		3
Walk Test End	378		3
Walk Test Start	379		3
Bus Device Missing	380		3
Bus Device Missing Restoral	381		3
Battery Missing	382		3
Battery Missing Restoral	383		3
RAM Checksum Failed	384		3

Global Report Routing Items

Programming Item	Item Number	Description (Range)	Entry
Communicator Disable	304	0 = Enable reporting 1 = Disable reporting (local-only system)	0
Route Attempts	305	Enter the number of times the system attempts each destination in the selected route if the first attempt fails (1 to 20). The system alternates between the primary and backup destinations. If both destinations are programmed for the selected route group, the number of attempts is doubled. For example, if this item is set to 10, the system tries the primary destination 10 times and the backup destination 10 times for a total of 20 attempts.	10
Send Reports During Walk Test	306	0 = No reports are sent during Walk Test 1 = Only Walk Test Start and Walk Test End reports are sent during Walk Test	0

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.5 Point Programming Items

Refer to the *Point Programming Entry Tables,* starting on page 47, for expert programming item numbers, default values, and programming entry cells.

<table>
<tr><th>Programming Item</th><th>Description (Range)</th></tr>
<tr><td>Point Type</td><td>Refer to Section 4.2.1 Points on page 31 for point type descriptions.
0 = Disabled
1 = Perimeter
2 = Interior
3 = Perimeter Instant
4 = 24-Hour
5 = Fire Verified*
6 = Fire Instant
7 = Silent Panic
8 = Interior Walkthrough
9 = Perimeter Exit Cancel
11 = Momentary Keyswitch
12 = Maintained Keyswitch
* This option is not available for wireless smoke detectors.</td></tr>
<tr><td>Circuit Style</td><td>0 = Dual 2.2 kΩ alarm and tamper circuit
2 = Single 2.2 kΩ alarm circuit</td></tr>
<tr><td>Include in Custom Protection</td><td>0 = Point not included in Custom Protection
1 = Point included in Custom Protection
Regardless of which protection mode is selected, 24-Hour, Fire Verified, Fire Instant, and Panic points always create alarm conditions if faulted.</td></tr>
<tr><td>Cross Zone Enabled</td><td>0 = Cross zoning disabled
1 = Cross zoning enabled
Do not change this item number's setting unless Expert Programming Item Number 124 = 1.
Refer to page 38 for more information.</td></tr>
<tr><td>Response Time</td><td>Sets the point's response time in 50 ms increments (1 to 10).
The value entered is multiplied by 50. For example, 6 x 50 = 300 ms response time.</td></tr>
<tr><td>Wireless Detector Sensitivity</td><td>Determines how long the detector must detect motion before generating an alarm. The lower this level is set, the longer the detector must detect motion before generating an alarm. This applies to the wireless motion detectors (PIR and dual) and inertia detector. This item also determines the inertia detector's pulse setting.
Motion Detector (PIR and dual)
0 = Standard
4 = Intermediate
Inertia Detector
<table><tr><th>Gross Attack Options</th></tr><tr><td>0 = Tap off, low sensitivity
1 = Tap off, low/medium sensitivity
2 = Tap off, medium/high sensitivity
3 = Tap off, high sensitivity</td></tr><tr><th>Minor Attack Options</th></tr><tr><td>8 = Tap on, 8 taps, low sensitivity
9 = Tap on, 8 taps, low/medium sensitivity
10 = Tap on, 8 taps, medium/high sensitivity
11 = Tap on, 8 taps, high sensitivity
12 = Tap on, 4 taps, low sensitivity
13 = Tap on, 4 taps, low/medium sensitivity
14 = Tap on, 4 taps, medium/high sensitivity
15 = Tap on, 4 taps, high sensitivity</td></tr></table></td></tr>
</table>

Point Programming Entry Tables

Point 1	Programming Item (Item Number)	Entry
	Point Type (9011)	6
	Circuit Style (9012)	2
	Include in Custom Protection (9013)	0
	Cross Zone Enabled (9014)	1
	Response Time (9015)	6
	Wireless Detector Sensitivity (9018)	0
	Voice Description	Point 1
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 5	Programming Item (Item Number)	Entry
	Point Type (9051)	1
	Circuit Style (9052)	2
	Include in Custom Protection (9053)	0
	Cross Zone Enabled (9054)	1
	Response Time (9055)	6
	Wireless Detector Sensitivity (9058)	0
	Voice Description	Point 5
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 2	Programming Item (Item Number)	Entry
	Point Type (9021)	1
	Circuit Style (9022)	2
	Include in Custom Protection (9023)	0
	Cross Zone Enabled (9024)	1
	Response Time (9025)	6
	Wireless Detector Sensitivity (9028)	0
	Voice Description	Point 2
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 6	Programming Item (Item Number)	Entry
	Point Type (9061)	2
	Circuit Style (9062)	2
	Include in Custom Protection (9063)	0
	Cross Zone Enabled (9064)	1
	Response Time (9065)	6
	Wireless Detector Sensitivity (9068)	0
	Voice Description	Point 6
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 3	Programming Item (Item Number)	Entry
	Point Type (9031)	1
	Circuit Style (9032)	2
	Include in Custom Protection (9033)	0
	Cross Zone Enabled (9034)	1
	Response Time (9035)	6
	Wireless Detector Sensitivity (9038)	0
	Voice Description	Point 3
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 7	Programming Item (Item Number)	Entry
	Point Type (9071)	2
	Circuit Style (9072)	2
	Include in Custom Protection (9073)	0
	Cross Zone Enabled (9074)	1
	Response Time (9075)	6
	Wireless Detector Sensitivity (9078)	0
	Voice Description	Point 7
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 4	Programming Item (Item Number)	Entry
	Point Type (9041)	1
	Circuit Style (9042)	2
	Include in Custom Protection (9043)	0
	Cross Zone Enabled (9044)	1
	Response Time (9045)	6
	Wireless Detector Sensitivity (9048)	0
	Voice Description	Point 4
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Point 8	Programming Item (Item Number)	Entry
	Point Type (9081)	2
	Circuit Style (9082)	2
	Include in Custom Protection (9083)	0
	Cross Zone Enabled (9084)	1
	Response Time (9085)	6
	Wireless Detector Sensitivity (9088)	0
	Voice Description	Point 8
	Wired (On-board) Wireless Point (Wireless Hub)	☐ Wired ☐ Wireless

Default = Default value.

Default = Country-specific default. Select this programming item to hear the updated default value.

Point 9	Programming Item (Item Number)	Entry
	Point Type (9091)	0
	Circuit Style (9092)	2
	Include in Custom Protection (9093)	0
	Cross Zone Enabled (9094)	1
	Wireless Detector Sensitivity (9098)	0
	Voice Description	Point 9
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 13	Programming Item (Item Number)	Entry
	Point Type (9131)	0
	Circuit Style (9132)	2
	Include in Custom Protection (9133)	0
	Cross Zone Enabled (9134)	1
	Wireless Detector Sensitivity (9138)	0
	Voice Description	Point 13
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 10	Programming Item (Item Number)	Entry
	Point Type (9101)	0
	Circuit Style (9102)	2
	Include in Custom Protection (9103)	0
	Cross Zone Enabled (9104)	1
	Wireless Detector Sensitivity (9108)	0
	Voice Description	Point 10
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 14	Programming Item (Item Number)	Entry
	Point Type (9141)	0
	Circuit Style (9142)	2
	Include in Custom Protection (9143)	0
	Cross Zone Enabled (9144)	1
	Wireless Detector Sensitivity (9148)	0
	Voice Description	Point 14
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 11	Programming Item (Item Number)	Entry
	Point Type (9111)	0
	Circuit Style (9112)	2
	Include in Custom Protection (9113)	0
	Cross Zone Enabled (9114)	1
	Wireless Detector Sensitivity (9118)	0
	Voice Description	Point 11
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 15	Programming Item (Item Number)	Entry
	Point Type (9151)	0
	Circuit Style (9152)	2
	Include in Custom Protection (9153)	0
	Cross Zone Enabled (9154)	1
	Wireless Detector Sensitivity (9158)	0
	Voice Description	Point 15
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 12	Programming Item (Item Number)	Entry
	Point Type (9121)	0
	Circuit Style (9122)	2
	Include in Custom Protection (9123)	0
	Cross Zone Enabled (9124)	1
	Wireless Detector Sensitivity (9128)	0
	Voice Description	Point 12
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 16	Programming Item (Item Number)	Entry
	Point Type (9161)	0
	Circuit Style (9162)	2
	Include in Custom Protection (9163)	0
	Cross Zone Enabled (9164)	1
	Wireless Detector Sensitivity (9168)	0
	Voice Description	Point 16
	Wired (DX2010 Address 102)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

* These options apply to the entire point range. These points cannot be individually configured.

Default = Default value.

Default = Country-specific default. Select this programming item to hear the updated default value.

Point 17	Programming Item (Item Number)	Entry
	Point Type (9171)	0
	Circuit Style (9172)	2
	Include in Custom Protection (9173)	0
	Cross Zone Enabled (9174)	1
	Wireless Detector Sensitivity (9178)	0
	Voice Description	Point 17
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 21	Programming Item (Item Number)	Entry
	Point Type (9211)	0
	Circuit Style (9212)	2
	Include in Custom Protection (9213)	0
	Cross Zone Enabled (9214)	1
	Wireless Detector Sensitivity (9218)	0
	Voice Description	Point 21
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 18	Programming Item (Item Number)	Entry
	Point Type (9181)	0
	Circuit Style (9182)	2
	Include in Custom Protection (9183)	0
	Cross Zone Enabled (9184)	1
	Wireless Detector Sensitivity (9188)	0
	Voice Description	Point 18
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 22	Programming Item (Item Number)	Entry
	Point Type (9221)	0
	Circuit Style (9222)	2
	Include in Custom Protection (9223)	0
	Cross Zone Enabled (9224)	1
	Wireless Detector Sensitivity (9228)	0
	Voice Description	Point 22
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 19	Programming Item (Item Number)	Entry
	Point Type (9191)	0
	Circuit Style (9192)	2
	Include in Custom Protection (9193)	0
	Cross Zone Enabled (9194)	1
	Wireless Detector Sensitivity (9198)	0
	Voice Description	Point 19
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 23	Programming Item (Item Number)	Entry
	Point Type (9231)	0
	Circuit Style (9232)	2
	Include in Custom Protection (9233)	0
	Cross Zone Enabled (9234)	1
	Wireless Detector Sensitivity (9238)	0
	Voice Description	Point 23
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 20	Programming Item (Item Number)	Entry
	Point Type (9201)	0
	Circuit Style (9202)	2
	Include in Custom Protection (9203)	0
	Cross Zone Enabled (9204)	1
	Wireless Detector Sensitivity (9208)	0
	Voice Description	Point 20
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 24	Programming Item (Item Number)	Entry
	Point Type (9241)	0
	Circuit Style (9242)	2
	Include in Custom Protection (9243)	0
	Cross Zone Enabled (9244)	1
	Wireless Detector Sensitivity (9248)	0
	Voice Description	Point 24
	Wired (DX2010 Address 103)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

* These options apply to the entire point range. These points cannot be individually configured.

Default = Default value.

Default = Country-specific default. Select this programming item to hear the updated default value.

Point 25	Programming Item (Item Number)	Entry
	Point Type (9251)	0
	Circuit Style (9252)	2
	Include in Custom Protection (9253)	0
	Cross Zone Enabled (9254)	1
	Wireless Detector Sensitivity (9258)	0
	Voice Description	Point 25
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 29	Programming Item (Item Number)	Entry
	Point Type (9291)	0
	Circuit Style (9292)	2
	Include in Custom Protection (9293)	0
	Cross Zone Enabled (9294)	1
	Wireless Detector Sensitivity (9298)	0
	Voice Description	Point 29
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 26	Programming Item (Item Number)	Entry
	Point Type (9261)	0
	Circuit Style (9262)	2
	Include in Custom Protection (9263)	0
	Cross Zone Enabled (9264)	1
	Wireless Detector Sensitivity (9268)	0
	Voice Description	Point 26
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 30	Programming Item (Item Number)	Entry
	Point Type (9301)	0
	Circuit Style (9302)	2
	Include in Custom Protection (9303)	0
	Cross Zone Enabled (9304)	1
	Wireless Detector Sensitivity (9308)	0
	Voice Description	Point 30
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 27	Programming Item (Item Number)	Entry
	Point Type (9271)	0
	Circuit Style (9272)	2
	Include in Custom Protection (9273)	0
	Cross Zone Enabled (9274)	1
	Wireless Detector Sensitivity (9278)	0
	Voice Description	Point 27
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 31	Programming Item (Item Number)	Entry
	Point Type (93011)	0
	Circuit Style (9312)	2
	Include in Custom Protection (9313)	0
	Cross Zone Enabled (9314)	1
	Wireless Detector Sensitivity (9318)	0
	Voice Description	Point 31
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 28	Programming Item (Item Number)	Entry
	Point Type (9281)	0
	Circuit Style (9282)	2
	Include in Custom Protection (9283)	0
	Cross Zone Enabled (9284)	1
	Wireless Detector Sensitivity (9288)	0
	Voice Description	Point 28
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

Point 32	Programming Item (Item Number)	Entry
	Point Type (9321)	0
	Circuit Style (9322)	2
	Include in Custom Protection (9323)	0
	Cross Zone Enabled (9324)	1
	Wireless Detector Sensitivity (9328)	0
	Voice Description	Point 32
	Wired (DX2010 Address 104)* Wireless Point (Wireless Hub)*	☐ Wired ☐ Wireless

* These options apply to the entire point range. These points cannot be individually configured.

Default = Default value.

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.6 Output Programming Items

Use Outputs 5 to 8 only for wireless output devices.

Programming Item	Item Number	Description	Entry
Fire Output Cadence	600	0 = Temporal Code 3 cadence 1 = Pulse cadence (two-sec on, two-sec off)	0
Output 1 Type	611	Refer to *Section 4.2.3 Outputs* on page 33 for output function descriptions. 0 = Output disabled 1 = Intrusion 2 = Intrusion Latching 3 = Fire 4 = Fire Latching 5 = Intrusion and Fire 6 = Intrusion and Fire Latching 7 = System Reset 8 = System On 9 = System Ready 10 = Key Fob On/Off 11 = Key Fob 2-sec Pulse 13 = User Controlled	5
Output 2 Type	621		5
Output 3 Type	631		7
Output 4 Type Supervised speaker driver option. Refer to *Expert Programming Item Number 642*.	641		5
Output 5 Type (wireless)	651		0
Output 6 Type (wireless)	661		0
Output 7 Type (wireless)	671		0
Output 8 Type (wireless)	681		0
Output 4 Function	642	0 = Supervised 8 Ω speaker driver 1 = Unsupervised open collector (voltage level)	0

Default = Country-specific default. Select this programming item to hear the updated default value.

When programming a wireless output (for example, a siren or relay module), do not select an output function that requires the output to activate for an extended period (for example System Ready).

4.3.7 Control Center Programming Items

Speech Configuration Items

Programming Item	Item Number	Description (Range)	Entry
Alarm Message Minimum Repeat Time	880	Enter how long the control center waits between alarm message announcements before repeating the message even if the control center's proximity sensor detects motion (1 to 255 hrs).	12
"No Alarm Report Sent" Announcement	883	0 = No announcement for aborted alarms. 1 = Control center announces "No alarm report sent" for aborted alarms.	1
"Cancel Report Sent" Announcement	884	0 = No announcement for canceled alarms. 1 = Control center announces "Cancel report sent" for cancelled alarms.	1
Time Format	887	0 = Determined by voice module 1 = Always use 12-hr mode 2 = Always use 24-hr mode	0

Global Control Center Items

These programming items affect all control centers connected to the control panel.

To send a user fire, emergency (medical) or panic report, the appropriate control center button and report must be enabled. Refer to *Section 4.3.4 Report Routing Programming Items* on page 43 to enable reports.

Check the appropriate box in the *Easy Series User Guide* (P/N: F01U025111) to identify which buttons are enabled.

Programming Item	Item Number	Description (Range)	Entry
Fire Button Alarm	888	0 = Item disabled. 1 = Press and hold [1] for 2 sec to start a fire alarm.	0
Medical Button Alarm	889	0 = Item disabled. 1 = Press and hold [1] and [2] for 2 sec to start a medical alarm. System announces medical alarm message once every minute for five min.	0
Panic Button Alarm	890	0 = Item disabled. 1 = Press and hold [2] for 2 sec to start an audible panic alarm. 2 = Press and hold [2] for 2 sec to start a silent panic alarm.	0
One Button Arming	891	0 = Token or passcode is required to turn the system on. 1 = Press [i] to start Exit Delay for the first available system-on option. No token or passcode is needed.	0
Invalid Passcode Attempt Limit	892	Enter the number of times a user can enter an invalid passcode, or present an invalid token, before the user is locked out (3 to 8).	3
Control Center Lockout Time	893	Enter the number of minutes that a user is locked out when the *Invalid Passcode Attempt Limit* is reached (1 to 30).	3

Individual Control Center Items

These programming items are set independently for each control center connected to the control panel.

Programming Item	Item Number	Description	Entry
Control Center Brightness	**Control Center 1:** 811	5 = Brightest display (1 to 5)	**Control Center 1:** 5
	Control Center 2: 821		**Control Center 2:** 5
	Control Center 3: 831		**Control Center 3:** 5
	Control Center 4: 841		**Control Center 4:** 5
Control Center Backlight Extinguish Mode	**Control Center 1:** 814	0 = Display is always on 1 = Display is dim until presence is detected or button is pressed 2 = Display is off until presence is detected or button is pressed 3 = Display is off until a valid token is presented or passcode is entered	**Control Center 1:** 0
	Control Center 2: 824		**Control Center 2:** 0
	Control Center 3: 834		**Control Center 3:** 0
	Control Center 4: 844		**Control Center 4:** 0

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.8 User Programming Items

Programming Item	Item Number	Description (Range)	Entry
Passcode Length	861	Set the length of all passcodes (4 or 6 digits).	4
Installer Passcode (User 0)	7001	**Four-digit Range:** 1111 to 5555 **Six-digit Range:** 111111 to 555555	5432 543211
Master User Passcode (User 1)	7011	**Four-digit Range:** 1111 to 5555 **Six-digit Range:** 111111 to 555555	1234 123455
Duress User (User 22) Enabled	862	0 = Duress user disabled 1 = Duress user enabled **Duress User passcode:** **Six digits:** 111111 **Four digits:** 1111	0
RFID Token Password	863	Use this item to prevent unauthorized copying of tokens (00000000 to FFFFFFFF). Do not change this item once tokens are added to the system.	12345678

Default = Country-specific default. Select this programming item to hear the updated default value.

4.3.9 Factory Default

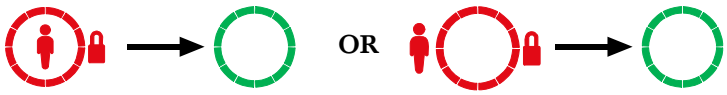
Programming Item	Item Number	Description
Factory Default	9999	Enter 9999 to restore all factory default values. All programming items, except for the country code, are reset when you restore the factory default values. This item also deletes all wireless data, but does not default the wireless hub.

4.4 Exit Programming

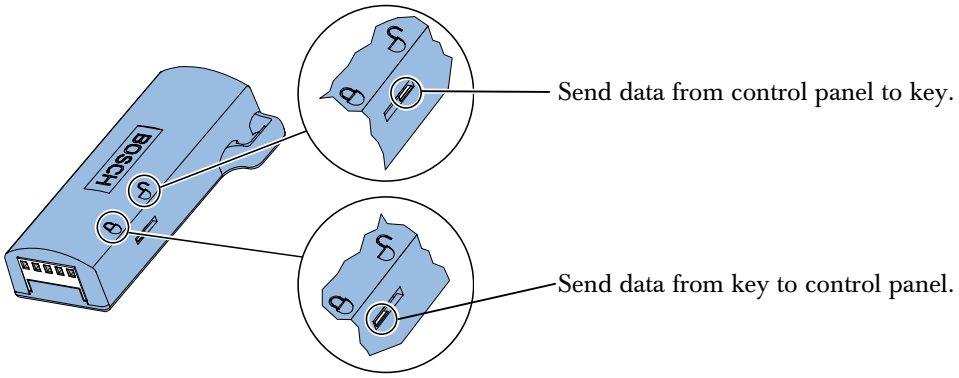
Press [#] repeatedly until the system says "goodbye." This ends the phone session.

4.5 Programming Key

1. If the system is on, turn it off.

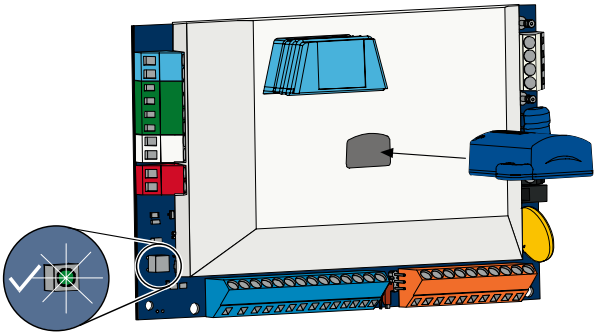


2. Place the key's lock switch in the desired position.



Verify the switch position before inserting the programming key into the control panel board. An incorrect switch position might overwrite programming data.

3. Insert the key into the control panel board.



- **Auto Transfer:** If *Expert Programming Item Number 123* = 1 (refer to *Programming Key Auto Transfer* on page 38), the programming key automatically transfers data depending on the position of the lock switch.
- **Manual Transfer:** If *Expert Programming Item Number 123* = 0, you must use the Installer Menu to access the programming key.

  The control center announces when data transfer is completed.

4. When the √ LED flashes green, data transfer is successful. If the √ LED flashes red, the data transfer is unsuccessful.

Bosch recommends that you transfer the programming data to the ICP-EZPK Programming Key when you finish programming the control panel.

4.6 Remote Programming Software (RPS)

There are two methods to start a session with the remote programming software (RPS): the installer calls RPS, or RPS calls the control panel.

Select the method that best meets the system's needs for remote programming.

RPS-to-control panel communication not investigated by UL.

At any time during a voice phone session between the installer and RPS operator, the RPS operator can start the remote programming session by selecting *Direct* as the connection method and clicking **Connect** on the RPS Panel Communication window.

4.6.1 Installer Calls RPS

1. From the house phone, the installer dials the RPS phone number.
2. At the site where the RPS PC is located, the RPS operator clicks **Answer** on the Panel Communication window. The control panel seizes the phone line, and the remote programming session starts.

4.6.2 RPS Calls the Control Panel

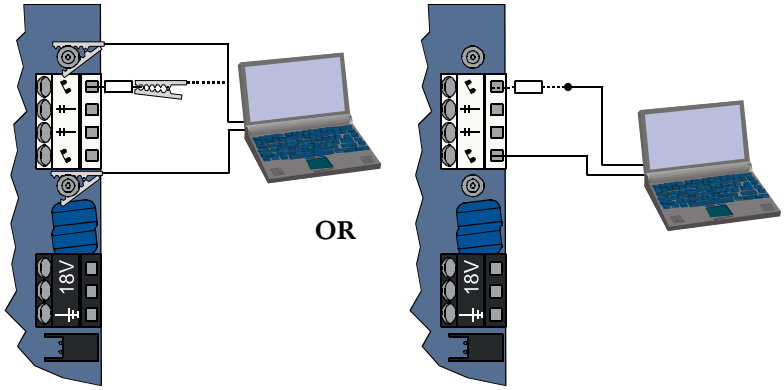
RPS can use either the public switched telephone network (PSTN) or a direct connection to call the control panel.

PSTN Option

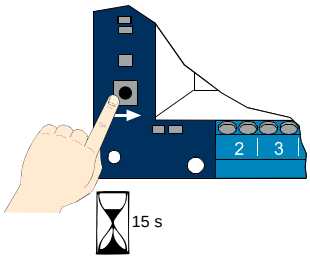
1. The RPS operator selects **Modem** as the connection method in the Panel Communication window, and then clicks **Connect**.
2. When the incoming call is answered, RPS sends the connection tone and the remote programming session starts.

Direct Connection

1. Connect the RPS PC or laptop to the control panel's house phone terminals.
   It might be necessary to connect a 270 Ω to 330 Ω, ¼ W resistor.



2. Press and hold the control panel's System Test button for approximately 15 seconds, or until the relay clicks.
3. From the RPS Panel Communication window, select *Direct* as the connection method and click **Connect**. The remote programming session starts.
4. At the end of the remote programming session, reconnect the PSTN line if it was disconnected in *Step 1*.



5.0 System Test

When the installation and programming of the control panel is complete, test the control panel and all devices for proper operation. Test the control panel after you first program it, and after any subsequent programming.

If you test a device and the control panel does not respond, check the device, its wiring, and any related settings or programming for potential errors.

To conduct a full system test, use either option:

Installer Menu

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. When prompted, enter the installer passcode.
3. Press [1] for System Maintenance.
4. Press [2] for Full System Test.

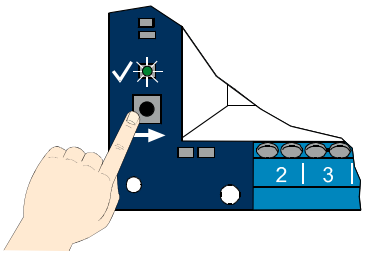
One-Button System Test

Press the System Test button on the control panel board once.

The system performs the same tests available on the Installer Menu.

√ LED green flash = test successful

√ LED red flash = test unsuccessful

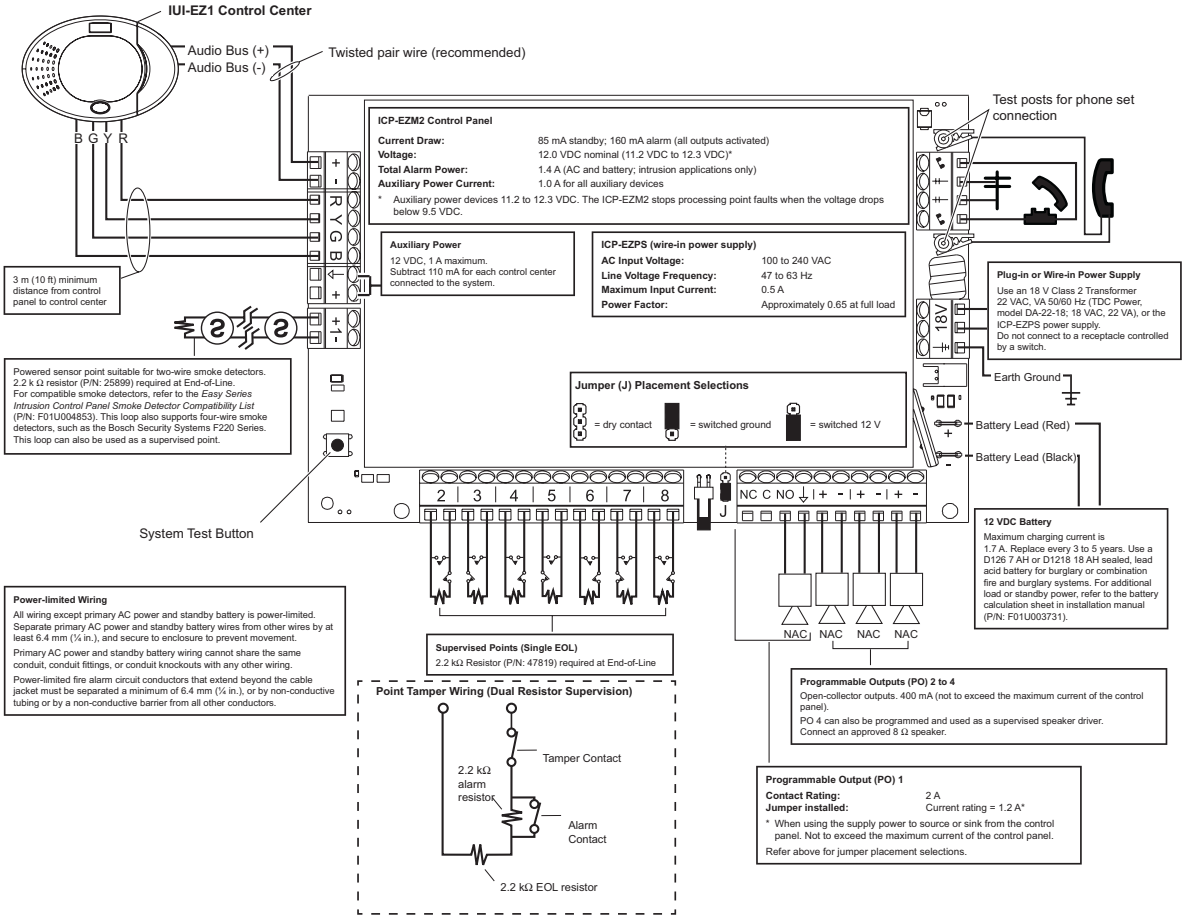


6.0 Maintenance

Bosch recommends testing the system regularly, and inspecting it according to local code or law.

7.0 Reference Materials

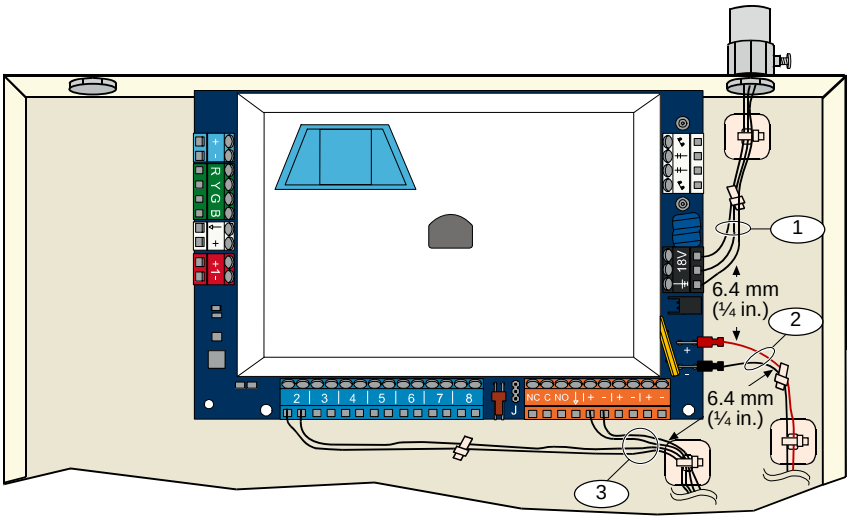
7.1 Enclosure Wiring Label



7.2 Power-limited Wire Routing

All wiring except primary AC power and standby battery is power-limited. Separate primary AC power and standby battery wires from other wires by at least 6.4 mm (¼ in.), and secure to enclosure to prevent movement.

Primary AC power and standby battery wiring cannot share the same conduit, conduit fittings, or conduit knockouts with any other wiring.



1 - Primary 18 VAC power wiring.
2 - Standby battery wiring.
3 - Power-limited point and output wiring.

7.3 Standby Battery Calculation

Use the following formula to calculate standby battery capacity for 24 hr of standby power and 4 to 30 minutes of alarm power:

(Total B _____ x 24 hr) + (Total C _____ x Y hr*) + 10% reserve = Total battery Ah required

* Y hr =

- For UL-approved residential applications (household), Y = 0.067 (4 minutes)
- For UL-approved commercial applications, Y = 0.25 (15 minutes)
- For ULC-approved commercial applications, Y = 0.50 (30 minutes)

If the Column C total exceeds 1.4 A, use an external power supply.

		A AC Power On Normal Current				**B AC Power Off Minimum Current**				**C In Alarm Maximum Current**			
Model Number	**Quantity Used**	**Each Unit (mA)**			**Total (mA)**	**Each Unit (mA)**			**Total (mA)**	**Each Unit (mA)**			**Total (mA)**
Control Panel		85	x 1	=	85	85	x 1	=	85	160	x 1	=	160
Control Center		110	x Qty	=		110	x Qty	=		165	x Qty	=	
Wireless Hub (IWT-WSN-N1-86)		30	x 1	=	30	30	x 1	=	30	30	x 1	=	30
DX2010		35	x Qty	=		35	x Qty	=		35	x Qty	=	
Sounders Connected to PO 4													
D118 8 Ω Speaker		0	x Qty	=	0	0	x Qty	=	0	330	x Qty	=	
Ratings of other devices in system that are not shown above													
			x Qty	=			x Qty	=			x Qty	=	
			x Qty	=			x Qty	=			x Qty	=	
			x Qty	=			x Qty	=			x Qty	=	
			x Qty	=			x Qty	=			x Qty	=	
			x Qty	=			x Qty	=			x Qty	=	
			x Qty	=			x Qty	=			x Qty	=	
			Total A	=			**Total B**	=			**Total C**	=	

7.4 Event Report Codes

Event	SIA Report	Contact ID Report
Intrusion Alarm	BA Burglary Alarm	1 130 Burglary
Intrusion Alarm Verified	BV Burglary Alarm Verified	1 139 Burglary
Intrusion Alarm Unverified	BG Unverified Event Burglary	1 130 Burglary
Intrusion Alarm 24-hr	BA Burglary Alarm	1 133 24 Hour (Safe)
Intrusion Alarm 24-hr Restoral	BH Burglary Alarm Restore	3 133 Restoral
Intrusion Alarm Restoral	BR Burglary Restoral	3 130 Burglary
Duress	HA Hold Up Alarm	1 121 Duress
Exit Error	EA Exit Alarm	1 374 Exit Error (zone)
Fire Alarm	FA Fire Alarm	1 110 Fire
Fire Alarm Unverified	FG Unverified Event-Fire	1 110 Fire
Fire Alarm Restoral	FH Fire Alarm Restore	3 110 Fire
Panic	HA Holdup Alarm	1 120 Panic
Panic Restoral	HH Holdup Alarm Restore	3 120 Panic
User Emergency (Medical)	QA Emergency Alarm	1 101 Personal Emergency
User Fire	FA Fire Alarm	1 110 Fire
User Fire Restoral	FH Fire Alarm Restore	3 110 Fire
User Panic	HA Holdup Alarm	1 120 Panic
Cancel	BC Burglary Cancel	1 406 Cancel
Intrusion Trouble	BT Burglary Trouble	1 380 Sensor Trouble
Intrusion Trouble Restoral	BJ Burglary Trouble Restore	3 380 Sensor Trouble
Intrusion Point Bypass	BB Burglary Bypass	1 570 Zone/Sensor bypass
Intrusion Point Bypass Restoral	BU Burglary Unbypass	3 570 Zone/Sensor bypass
Fire Trouble	FT Fire Trouble	1 373 Fire Trouble
Fire Trouble Restoral	FJ Fire Trouble Restore	3 373 Fire Trouble
Recent Closing	CR Recent Closing	1 459 Recent Closing
Close (System On) Unoccupied	CL Closing Report	3 401 Unoccupied Arm by User
Close (System On) Occupied	CL Closing Report	3 441 Occupied Arm by User
Close (System On) Custom	CL Closing Report	3 441 Custom Arm by User
Close (System On) Partial	CL Closing Report	3 456 Partial Arm by User
Close (System On) Keyswitch	CS Closing Keyswitch (User 255)	3 409 Keyswitch O/C (User 255)
Open (System Off)	OP Opening Report	1 401 O/C by User
Open (System Off) Keyswitch	OS Opening Keyswitch (User 255)	1 409 Keyswitch O/C (User 255)
AC Fail	AT AC Trouble	1 301 AC Loss
AC Fail Restoral	AR AC Restoral	3 301 AC Loss
Auto System Test (Normal)	RP Automatic Test	1 602 Period Test Report (User 0)
Auto System Test (Off-Normal)	RY Test Off Normal	1 608 Period Test Report, System Trouble Present
Auxiliary Power Fault	IA Equipment Failure Condition	1 310 Ground Fault
Auxiliary Power Restoral	IR Equipment Fail Restoral	3 310 Ground Fault
Communication Fail	YC Communications Fail	1 354 Failure to communicate event
Communication Restoral	YK Communications Restoral	3 354 Failure to communicate event
Control Center Supervision Fail	EM Expansion Device Missing	1 333 Expansion module failure
Control Center Supervision Restoral	EN Expansion Missing Restore	3 333 Sensor Trouble
Control Center Tamper	ES Expansion Device Tamper	1 341 Expansion Device Tamper
Control Center Tamper Restoral	EJ Expansion Device Tamper Restore	3 341 Expansion Device Tamper
Local Programming	LX Local Programming Ended	1 628 Program mode exit
Low Battery	YT System Battery Trouble	1 302 Low System Battery
Low Battery Restoral	YR System Battery Restoral	3 302 Low System Battery
Communication Test	RX Manual Test	1 601 Manual trigger test report
Phone Line Fault	LT Phone Line Trouble	1 351 Telco 1 fault
Phone Line Fault Restoral	LR Phone Line Restoral	3 351 Telco 1 fault

Event	SIA Report	Contact ID Report
ROM Fault	YF Parameter Checksum Fail	1 304 ROM Checksum Bad
Bell Trouble	YA Bell Fault	1 320 Sounder/ Relay
Bell Restoral	YH Bell Restored	3 320 Sounder/ Relay
Walk Test End	TE Test End	3 607 Walk Test Mode
Walk Test Start	TS Test Start	1 607 Walk Test Mode
Bus Device Missing	EM Expansion Device Missing	1 333 Exp. Module Failure
Bus Device Missing Restoral	EN Expansion Missing Restore	3 333 Exp. Module Failure
Battery Missing	YM System Battery Missing	1 311 Battery Missing/Dead
Battery Missing Restoral	YR System Battery Restoral	3 311 Battery Missing/Dead
RAM Checksum Failed	YF Parameter Checksum Fail	1 303 RAM Checksum bad
Point Tamper	TA Tamper Alarm	1 137 Tamper
Point Tamper Restoral	TH Tamper Alarm Restoral	3 137 Tamper Restoral
Cross Zone Trouble	BG Unverified Event - Burglary	1 378 Cross-zone Trouble
Cross Zone Trouble Restoral	BR Burglary Restoral	3 378 Cross-zone Trouble
Point Missing	UY Untyped Missing Trouble	1 381 Loss of Supervision – RF
Point Missing Restoral	UJ Untyped Trouble Restore	3 381 Loss of Supervision – RF
Wireless Point Low Battery	XT Transmitter Battery Trouble	1 384 RF Low Battery
Wireless Point Low Battery Restoral	XR Transmitter Battery Restoral	3 384 RF Low Battery
Wireless Receiver Jammed	XQ RF Interference	1 344 RF Receiver Jam Detect
Wireless Receiver Jammed Restoral	XH RF Interference Restoral	3 344 RF Receiver Jam Detect
Bus Device Tamper	XS RF Receiver Tamper	1 341 Exp Module Tamper
Bus Device Tamper Restoral	XJ RF Receiver Tamper Restoral	3 341 Exp Module Tamper
Bus Device Trouble	ET Expansion Trouble	1 330 System Peripheral Trouble
Bus Device Trouble Restoral	ER Expansion Restoral	3 330 System Peripheral Trouble
Remote Programming Success	RS Remote Program Success	1 628 Program mode exit
Remote Programming Failure	RU Remote Program Fail	1 628 Program mode exit

The following table shows:

- Non-standard event messages that appear in the history log, and
- Event messages for SMS Text and Voice formats

Event	History Log Entry	SMS Text Format	Voice Format
Tamper Enclosure	Tamper 0	Point Trouble 0	Tamper 0
Duress	Duress; System Off User 22	Intrusion Alarm System Off	Duress System Off User 22
Quick Arm	System On Occupied User 0 System On Unoccupied User 0 System On Custom User 0	System On User 0	System On Occupied User 0 System On Unoccupied User 0 System On Custom User 0
Keyswitch On	System On Unoccupied 255	System On User 255	System On Unoccupied 255
Keyswitch Off	System Off 255	System Off User 255	System Off 255
Recent Close	Recent Close User X	Intrusion Alarm	Recent Close User X

7.5 Display States

	Display	Color	Description
System Off		Green circle	No alarm or trouble conditions exist. You can turn on the system.
		Flashing green circle	System trouble exists. You can still turn on the system. Alarm memory active.
		Flashing amber circle	System trouble exists. You cannot turn on the system. Alarm memory active.
		Broken green circle	Wired point(s) are faulted. Turn on the system to bypass faulted point(s). Chime point faulted. Chime tone sounds.
		Broken amber circle	Wired point(s) are faulted. You cannot turn on the system.
		Broken red circle; flashing red icons	Fire or intrusion alarm occurred.
		Single rotating segment	Alarm memory announcement. Add or change user token. Waiting for information from wireless network.
		Green circle and icons	Add or change user passcode. Outside icon appears for first passcode entry. Inside icon appears for second passcode entry.
		Green or amber	Point walk test. Green single circle segments represent tested points.
		Green flashing icons	Control center test. Icons alternately flash.

	Display	Color	Description
System On (Occupied or Custom Protection)		Flashing red icon	Exit Delay in progress. Circle segments turn on, one at a time, to provide a visual status of Exit Delay.
		Red	System is on (occupied or custom protection).
		Flashing icon (amber then red)	Entry Delay in progress. Circle segments turn off, one at a time, to provide a visual status of Entry Delay. Amber icon: First half of Entry Delay Red icon: Second half of Entry Delay
		Broken red circle; flashing red icons	Fire or intrusion alarm occurred.
		Flashing red circle	Active alarm memory (if system is on).
		Single red rotating segment	Alarm memory announcement (if system is on).
System On (Unoccupied)		Flashing red icon	Exit Delay in progress.
		Red	System is on (unoccupied).
		Flashing icon (amber then red)	Entry Delay in progress. Amber icon: First half of Entry Delay Red icon: Second half of Entry Delay
		Broken red circle; flashing red icons	Fire or intrusion alarm occurred.
		Flashing red circle	Active alarm memory (if system is on).
		Single red rotating segment	Alarm memory announcement (if system is on).

7.6 Frequently Asked Questions (FAQ)

7.6.1 Programming Questions

Can I program the control panel if I do not have a phone line connected to it?

Yes. Follow these steps:

1. Connect a phone set to the phone set posts on the control panel board.
2. Press and hold the system test button for approximately 15 sec.
3. Enter the installer passcode when prompted.

The emergency buttons on the control center do not work. How do I activate them?

By default, the emergency buttons are turned off. Follow these steps to turn them on:

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. Enter the installer passcode.
3. Press [4] to select Expert Programming.
4. Enter the following expert programming item numbers, and change the setting for each button:
   - 888 = fire alarm (0 = disabled, 1 = fire alarm)
   - 889 = medical alarm (0 = disabled, 1 = medical alarm)
   - 890 = panic alarm (0 = disabled, 1 = audible panic alarm, 2 = silent panic alarm)
5. Ensure that the following reports are enabled:
   - 319 = user emergency (1 = Route 1 only, 2 = Route 2 only, 3 = both routes)
   - 320 = user fire (1 = Route 1 only, 2 = Route 2 only, 3 = both routes)
   - 322 = user panic (1 = Route 1 only, 2 = Route 2 only, 3 = both routes)
6. Press [#] repeatedly until you hear the system say “goodbye.” The buttons are now active.

How do I program a duress passcode?

Follow these steps:

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. Enter the installer passcode.
3. Press [4] to select Expert Programming.
4. Press [8][6][2] to select *Expert Programming Item Number 862*, and then press [1] to enable the duress user (User 22).
   By default, the duress passcode is “1111” if the passcode length = 4 digits, or “111111” if the passcode length = 6 digits.
5. Press [#] until you hear the system say “goodbye.”
6. Start a new phone session.
7. Enter the master user passcode.
8. Press [4] to select the User Menu.
9. Press [2] to change a user.
10. Press [2] repeatedly to scroll through all available users until you reach User 22.
11. Press [1] to select User 22.
12. Press [3] to enter a new passcode.
13. Enter a new passcode. Only digits 1 through 5 are allowed.
    You cannot assign a token to User 22.
14. Press [1] to return to User Menu selections.
15. Press [#] repeatedly until you hear the system say “goodbye.”
    The duress user (User 22) is now active.

I want to use the Custom Protection feature. How do I turn it on?

Follow these steps:

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. Enter the installer passcode.
3. Press [4] to select Expert Programming.
4. Enter the appropriate expert programming item number.
   Use *Expert Programming Item Numbers 9013* to *9323* to set the Custom Protection option for each desired point. The middle digits = the point number. For example, "01" = Point 1, and "32" = Point 32.
   - For Point 1, press [9][0][1][3].
   - For Point 2, press [9][0][2][3].
   - For Point 3, press [9][0][3][3].
   - For Point 10, press [9][1][0][3].
   - For Point 20, press [9][2][0][3].
   - For Point 32, press [9][3][2][3].
5. Press [1] to include the point in Custom Protection.
   24-Hour, Fire Verified, Fire Instant, and Panic points always create alarm conditions regardless of the selected protection mode.
6. Repeat *Steps 4* and *5* to include additional points in Custom Protection.
7. Press [#] repeatedly until you hear the system say "goodbye."
   Custom Protection is now an active protection mode selection. Only the points selected in *Steps 4* and *5* turn on when you turn on the system in Custom Protection mode.
   Custom protection points also turn on when you turn on the system as either Occupied or Unoccupied.

7.6.2 System Operation Questions

Will the system work if the voice module is different than the programmed country code?

Yes. The voice module operates independently from the programmed country code.

How do I add a user or token or key fob?

Only the master user can add a user or token or key fob.

From the control center:

1. Press and hold [3].
2. When asked, present the master user token or enter the master user passcode.
3. Press [1] to add a new user.
4. Enter a passcode. Re-enter the new passcode when asked.
   The system announces that the passcode was added.
5. Press [1] to add a token to the new user.
6. Present the token to the control center when asked.
   The system announces that the token was added.
7. Press [2] to record a user description (optional).
8. Press [4] to add a key fob (optional).
9. Repeat *Steps 3* to *8* to add more users and tokens, or press [5] to exit.

From a phone:

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. When asked, enter the master user passcode.
3. Press [4] to select the User Menu.
4. Follow *Steps 3* to *8* above to add users and tokens, or press [#] to exit.

If you are the master user and you cannot enter the User Menu when you present your token, you must assign your token as the master user token. Use the master user passcode to enter the User Menu, and then assign a token to yourself.

My token does not work when I present it to the control center. How do I fix this?

Your token is not assigned to you. If you are not the master user, see the master user.

If you are the master user, refer to the previous question for instructions on adding a token to a user.

How do I delete a user?

Only the master user can delete a user.

From the control center:

1. Press and hold [3].
2. When prompted, present the master user token or enter the master user passcode.
3. Press [3] to delete a user.
4. To select the first available user (not the master user), press [1]. To select a different user, press [2].
   Repeat this step until you select the desired user.
5. Press [1] to delete the user.
   The system announces that the user was deleted.
   The voice description is not deleted. Record a new description for a user that replaces the deleted user.
6. Repeat *Steps 4* and *5* to delete more users, tokens, and key fobs, or press [5] to exit.

From a phone:

1. Start a phone session. Refer to *Section 1.3 Basic Operation* Information on page 4 for instructions.
2. When prompted, enter the master user passcode.
3. Press [4] to select the User Menu.
4. Follow *Steps 3* to *5* above to delete users and tokens, or press [#] to exit.

To delete only a token:

1. Delete the user (follow either procedure shown above).
2. Add the user, but skip the step to assign a token or key fob.
   Follow either procedure shown in "How do I add a user or token or key fob?" on page 65.

I assigned a token to User 1 (Master User). Can I delete this token?

No. Once a token is assigned to User 1, User 1 always requires a token. The token cannot be deleted.

How do I replace a user's lost token or key fob?

1. Save the user's passcode (record it elsewhere).
2. Access the User Menu from either the control center or the User Phone Menu.
   Refer to *Section 1.2 Control Center Overview* on page 3, or *Section 1.3 Basic Operation Information* on page 4, for more information.
3. Delete the user.
4. Re-enter the user (use saved passcode).
5. Add the new token or key fob.

How do I reset a fire point?

1. To silence the alarm, present your token to the control center, or enter your passcode.
2. Repeat *Step 1* to reset the fire point.
   This procedure applies to any fire point type, such as a smoke detector, heat detector, or pull station.

How do I configure a four-wire smoke detector?

Connect the smoke detector's power wires to any programmable output. Then select "System Reset" for the output's function.

Can I reset an emergency alarm?

No. When an emergency alarm starts (press and hold both [1] and [2] keys on control center), the system announces an emergency alarm message once every minute for five minutes.

Can I turn the system on if there is a malfunction, such as a loss of main power?

Yes. Present your token twice to the control center.

Why do I hear the siren beep during Entry Delay?

Graduated Annunciation (*Expert Programming Item Number* 148) is enabled. If this item is enabled, the outputs periodically activate during Entry Delay to remind you to turn your system off.

Why does the siren activate during a Panic alarm?

Panic alarm is programmed for audible alarm.
In expert programming, change *Expert Programming Item Number 890* from 1 (audible alarm) to 2 (silent alarm).

My history log and central station report show Point 0 and User 0. What are these?

Point 0 = on-board input for EZTS tamper switch.
User 0 = installer.

7.6.3 Control Center Questions

How do I set the control center's address?

On the control center's printed circuit board, turn the rotary switch to the desired position (1 to 4). Each control center must have a unique address.

The control center does not initialize. All I see is a flashing amber circle.

Ensure that the rotary address switch on the control center's printed circuit board is properly set and not halfway between two numbers. Also, ensure that each control center has a unique address from 1 to 4.

The control center does not recognize any of my tokens.

If you have more than one control center, they are mounted too close to each other.
Ensure that there is at least 1.2 m (4 ft) between each control center.

Ensure that you do not run two or more sets of control center wiring together. Also, ensure that you do not coil extra control center wiring inside of the control panel's enclosure.

If you have more than one token on a keychain, separate the tokens. Tokens that are too close to one another interfere with control center operation.

The control center beeps when I present a token, but nothing else happens.

Your token is unassigned. If you are the master user, enter the master user passcode, select the User Menu, and assign a token to yourself. For all other users with this problem, the master user must enter the User Menu and assign a token to the appropriate user(s).

7.6.4 Passcode Questions

What are the default installer and master user passcodes?

- **Default installer passcode:** 5432 when passcode length = four digits; 543211 when passcode length = six digits
- **Default master passcode:** 1234 when passcode length = four digits; 123455 when passcode length = six digits

I cannot enter the Installer Menu using the installer passcode.

Expert Programming Item Number 142, *Restrict Installer Passcode*, is enabled. The master user must first present his or her token, or enter his or her passcode, before you enter the installer passcode. The Installer Passcode is enabled until a user turns the system on.

7.7 Agency Approvals and Requirements

7.7.1 Certifications and Approvals

Compliance with specific standards, such as SIA CP-01 and DD243, reduces false alarms and is required in many locations.

The Easy Series Intrusion Control Panel is designed to comply with the following certifications, approvals, and standards:

- ANSI/SIA CP-01 False Alarm Immunity
- CE
- EN50131-1 Security Grade 2, Environmental Class II*
- DD243*
- PD6662*
- CCC*
- UL Standards:
  - UL365, Police Station Burglar Alarm Units and Systems
  - UL609, Local Burglar Alarm Units and Systems
  - UL985, Household Fire Warning System Units
  - UL1023, Household Burglar-alarm System Units
  - UL1076, Proprietary Burglar Alarm Units and Systems
- cUL Standards:
  - CAN/ULC-S304-M88, Central and Monitoring Station Burglar Alarm Units
  - CAN/ULC-S545, Residential Fire Warning System Control Units
  - C1023, Household Burglar Alarm Units
  - CAN/ULC-S303, Local Burglar Alarm Units and Systems
  - C1076, Proprietary Burglar Alarm Units and Systems
- FCC
- Industry of Canada (IC)
- A-Tick*
- C-Tick*
- TBR21 for PSTN*
- INCERT (Belgium) *
- CSFM Listing – Control Unit Household
- Japan Approvals Institute for Telecommunications Equipment (JATE) *

* Not investigated by Underwriters Laboratories, Inc.

7.7.2 FCC

Part 15

This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy. If this equipment is not installed and used according to this document, it might cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user must correct the interference.

Part 68

This equipment complies with Part 68 of FCC rules. A label contains, among other information, the FCC registration number and ringer equivalency number (REN). If requested, this information must be provided to the telephone company.

The Bosch Security Systems Easy Series Intrusion Control Panel is registered for connection to the public telephone network using an RJ38X or RJ31X jack.

The REN determines the number of devices that can be connected to the telephone line. Excessive REN's on the telephone line might result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five. To determine the number of devices that can be connected to the telephone line, contact the telephone company for the maximum REN for the calling area.

The telephone company notifies you if this equipment harms the telephone network. If advance notice is not practical, the telephone company notifies the customer as soon as possible. Also, you are advised of your right to file a complaint with the FCC if you believe it is necessary to do so.

The telephone company might make changes in its facilities, equipment, operation, or procedures that could affect the operation of this equipment. If this happens, the telephone company provides advance notice so you can make the necessary modifications for maintaining uninterrupted service.

If you experience trouble with the Easy Series Intrusion Control Panel, contact Bosch Security Systems Customer Service for repair and warranty information. If the trouble harms the telephone network, the telephone company might request that you remove the equipment from the network until the problem is resolved. User repairs must not be made, and doing so voids the user's warranty.

This equipment cannot be used on public coin service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact your state public utilities commission for more information.

- **FCC Registration Number:** US:ESVAL00BEZ1; **Ringer Equivalence:** 0.0B
- **Service Center:** Contact your Bosch Security Systems representative for the location of your service center.

7.7.3 Industry Canada

This product meets the applicable Industry Canada technical specifications.

The ringer equivalence number (REN) for this terminal equipment is 0.0. The REN assigned to each terminal equipment indicates the maximum number of terminals allowed to be connected to a telephone interface. The termination of an interface can consist of any combination of devices subject only to the requirement that the sum of the REN of all devices does not exceed five.

7.7.4 SIA

Programming Requirements

To comply with ANSI/SIA CP-01 False Alarm Reduction, set these programming items as follows:

Programming Item	Item Number	Default	Page Reference
Intrusion Abort Window	110	30 sec	37
Intrusion Cancel Window	112	5 min	37
Exit Delay	126	60 sec	38
Entry Delay	127	30 sec	38
Exit Time Restart	128	1	38
Swinger Bypass Count	131	1	39
Auto Protection Level	132	1	39

* The middle digits = the point number. For example, "01" = Point 1, and "32" = Point 32.

To comply with ANSI/SIA CP-01 False Alarm Reduction, by default, this system:

- Sends Intrusion Alarm Verified and Exit Error reports
- Sends a Recent Closing report for any alarm that occurs within two min of the end of Exit Delay
- Includes a Fire Verified point type option that is disabled by default

Quick Reference

Refer to the following table for programmable features, shipping defaults, and recommended programming that comply with the ANSI/SIA CP-01 False Alarm Reduction standard.

The system test button tests all points, all outputs, the control panel, and the communicator. Refer to *Section 5.0 System Test* on page 56 for more information.

Paragraph Number in ANSI/SIA CP-01	Feature	Requirement	Range	Shipping Default	Recommended Programming[1]
4.2.2.1	Exit Time	Required (programmable)	For full or auto arming: 45 sec to 2 min (255 sec max)	60 sec	60 sec
4.2.2.2	Progress Annunciation/ Disable for Silent Exit	Allowed	Individual control centers can be disabled.	All control centers enabled.	All control centers enabled.
4.2.2.3	Exit Time Restart	Required option	For re-entry during Exit Time	Enabled	Enabled
4.2.2.5	Auto Stay Arm on Unvacated Premises	Required option (except for remote arm)	If no exit after full arm	Enabled	Enabled
4.2.4.4	Exit Time and Progress Annunciation/ Disable for Remote Arm	Allowed option (for remote arm)	Can be disabled for remote arm	Enabled	Enabled
4.2.3.1	Entry Delay(s)	Required (programmable)	30 sec to 4 min[2]	30 sec	At least 30 sec[2]
4.2.5.1	Abort Window for Non-fire Zones	Required option	Can be disabled by zone or zone type	Enabled	Enabled (all zones)
4.2.5.1	Abort Window Time for Non-fire Zones	Required (programmable)	15 sec to 45 sec[2]	30 sec	At least 15 sec[2]
4.2.5.1.2	Abort Annunciation	Required option	Annunciate that no alarm was transmitted	Enabled	Enabled
4.2.5.4.1	Cancel Annunciation	Required option	Annunciate that a Cancel was transmitted	Enabled	Enabled
4.2.6.1 and 4.2.6.2	Duress Feature	Allowed option	No 1+ derivative of another user code; no duplicates of other user codes	Disabled	Disabled
4.3.1	Cross Zoning	Required option	Programming needed	Disabled	Enabled and two or more zones programmed
4.3.1	Programmable Cross Zoning Time	Allowed	Can program	Per manufacturer	Per walk path in protected premises
4.3.2	Swinger Shutdown	Required (programmable)	For all non-fire zones, shut down at one or two faults	One fault	One fault
4.3.2	Swinger Shutdown Disable	Allowed	For non-police response zones	Enabled	Enabled (all zones)
4.3.3	Fire Alarm Verification	Required option	Depends on control panel and sensors	Disabled	Enabled unless sensors can self-verify
4.5	Call Waiting Cancel	Required option	Depends on user phone line	Disabled	Enabled if user has call waiting

[1] Programming at installation site might be subordinate to other UL requirements for the intended application.

[2] Combined Entry Delay and Abort Window should not exceed 1 minute.

[3] If the cross zone timer ends and a second cross zone point is not faulted, the system sends an intrusion alarm unverified report.

7.7.5 Underwriters Laboratories (UL)

Household Fire Warning System

- Install at least one UL Listed four-wire latching type smoke detector rated to operate over the voltage range of 11.2 VDC to 12.3 VDC. The maximum smoke detector load is 50 mA.
- Install one UL Listed 85 dB audible device rated to operate over the range of 11.2 VDC to 12.3 VDC as required for this application. Program the bell cut-off time for at least four minutes. Refer to *Programming Item 107* on page 37.
- Install end-of-line resistor P/N: 47819 after last smoke detector.
- Do not use a printer interface module.
- Where two-wire addressable devices are used, do not place fire and intrusion devices on the same zone.
- The system must be able to operate for at least 24 hr, and generate a full alarm output for at least 4 min without AC power.

Household Burglar Alarm Unit

- Install at least one UL Listed 85 dB audible device rated to operate over the voltage range of 11.2 VDC to 12.3 VDC.
- Install at least one IUI-EZ1 Control Center.
- Program all zones to use end-of-line supervision.
- Install intrusion initiating devices rated to operate over the voltage range of 11.2 VDC to 12.3 VDC.
- Program all intrusion zones for audible notification.
- Do not exceed 60 sec when programming Exit Delay. Refer to *Programming Item 126* on page 38. Do not exceed 45 sec when programming Entry Delay. Refer to *Programming Item 127* on page 38.
- Program the bell cut-off time for at least of four minutes. Refer to *Programming Item 108* on page 37.
- The system must be able to operate for at least 24 hr, and generate a full alarm output for at least 4 min without AC power.

Commercial Burglary, Local

- Use the D8108A Attack Resistant Enclosure with the D2402 Mounting Skirt.
- Install at least one UL Listed 85 dB audible device rated to operate over the voltage range of 11.2 VDC to 12.3 VDC. All wiring connections between the control panel and device must be in conduit.
- Do not exceed 60 sec when programming Exit Delay. Refer to *Programming Item 126* on page 38. Do not exceed 60 sec when programming Entry Delay. Refer to *Programming Item 127* on page 38.
- Install a tamper switch to protect the enclosure door.
- Set *Programming Item 116* to 1 (Daily) to ensure the automatic test report is sent on a daily basis. Refer to page 37.
- Ensure that the integrated communicator is enabled (*Programming Item 304* = 0; refer to page 45). Ensure that the system can send low battery reports (*Programming Item 358* = 1, 2, or 3; refer to page 45).
- Install at least one IUI-EZ1 Control Center.
- Program the bell cut-off time for at least 15 minutes. Refer to *Programming Item 108* on page 37.
- This system was not evaluated for Bank Safe and Vault applications.
- The system must be able to operate for at least 24 hr, and generate a full alarm output for at least 15 min without AC power.

Commercial Burglary, Police Station Connected Protected Premises*

- Refer to *Commercial Burglary, Local* for installation requirements.
- Ensure that the integrated communicator is enabled (*Programming Item 304* = 0; refer to page 45).

Commercial Burglary, Proprietary*

- The integrated communicator is enabled (*Programming Item 304* = 0; refer to page 45).
- The system has one owner.
- The system must be able to operate without AC power for at least 24 hours. The central station receiver must be able to receive reports without AC power for at least 24 hours.

* Systems are approved for Encrypted Line Security when used in conjunction with the C900V2 Conettix IP Dialer Capture Module and communicating over a packet-switched data network (PSDN).

7.7.6 EN50131-1

The Easy Series Intrusion Control Panel is designed to comply with EN50131-1 Security Grade 2, Environmental Class II.

Installation, Programming, and Maintenance
• **Installation:** Refer to *Section 2.0 Installation* on page 8. • **Programming:** Refer to *Section 4.0 Programming* on page 29. • **Testing:** Refer to *Section 5.0 System Test* on page 56. • **Maintenance:** Refer to *Section 6.0 Maintenance* on page 56.
Power Supply (AC and Standby Battery)
• **AC Power Supply:** Refer to *EZPS Power Supply Requirements* on page 75. • **Standby Battery:** Refer to *Control Panel Power Requirements* on page 75.
Automatic Inhibit
• **Intruder Alarm and Fault Signal or Message:** Set *Expert Programming Item Number 131* to a value between 1 and 3. Refer to page 39 for more information. • **Authorization Code:** Set *Expert Programming Item Number 892* to a value between 3 and 8. Refer to page 52 for more information.
Logical and Physical Keys
• **Minimum Number of Combinations per User:** - **Passcodes:** 15,625 (passcode length must be six digits) - **Tokens:** 42,000,000,000 - **Key Fobs:** 2,800,000,000,000,000 • **Method Used to Determine Number of Combinations:** - **Passcodes:** Digits 1 to 5 are allowed. For a six-digit passcode, all combinations are allowed. - **Tokens:** 32 bits. All combinations are allowed. - **Key Fobs:** 56 bits (48 serialized during manufacturing, 8 remain static)
Operating Temperature Range
Refer to *Environmental Considerations* on page 74.
Control Panel and Control Center Current Consumption
• **Control Panel:** Refer to *Control Panel Power Requirements* on page 75. • **Control Center:** Refer to *Control Center* on page 74.
Output Current Rating
Refer to Programmable Outputs on page 74.

To comply with EN50131-1, set these programming items as follows:

Programming Item	Item Number	Setting	Page Reference
Entry Delay	127	Set to 45 sec or less	38
Swinger Bypass Count	131	Select Option 3	39
Restrict Installer Passcode	142	Select Option 1	39
Passcode Length	861	Set passcode length to six digits	53

7.7.7 PD6662 and DD243 Requirements

To comply with PD6662 and DD243, you must meet all of the EN50131-3 requirements and the following requirements:

Maintenance
A qualified technician must check the system at least twice a year.
AC Power Supply
• **Type:** A • **Rated Voltage:** 230 V • **Rated Input Frequency:** 50 Hz • **Rated Input Current:** 250 mA maximum • **Fuse Rating:** 0.25 A, 250 V Slow Blow
Construction Material
Enclosures and housings for the control panel, control center, DX2010, wireless hub, and wireless devices are made from materials that are durable, secure, and resistant to attack by hand-held tools.
Confirmed Alarms
Set *Expert Programming Item Number 124* to either Option 3 or 4. Refer to page 38 for more information.

The Easy Series Intrusion Control Panel is designed to comply with PD6662:2004 as a Grade 2 system that supports Notification Options A, B, C, or X with the appropriate notification devices installed (devices not included with system).

7.7.8 INCERT

To comply with INCERT, set these programming items as follows:

Programming Item	Item Number	Default	Page Reference
Restrict Installer Passcode	142	1	39
Passcode Length	861	6 digits	53
Invalid Passcode Attempt	892	3*	52
Control Center Lockout Time	893	3*	52

* To comply with INCERT, set these programming items to 3 or higher.

7.7.9 cUL

For Canadian installations, install systems according to ULC-S302. Systems that use the C900V2 Conettix IP Dialer Capture Module meet Level 3 Line Security when communicating over a packet-switched data network (PSDN).

7.8 Specifications

Enclosure	
Dimensions (H x W x D):	37 cm x 31.8 cm x 8.5 cm (14.5 in. x 12.5 in. x 3.4 in.)
Construction Material:	Cold-rolled steel, zinc seal, 0.36 mm thick (20 Ga.)
Environmental Considerations	
Relative Humidity:	93% at 32°C ± 2°C (+90°F ± 2°F)
Operating Temperature:	-10°C to +49°C (+14°F to +120°F) • **UL:** 0°C to +49°C (+32°F to +120°F) • **CE:** -10°C to +40°C (+14°F to +104°F)
Storage Temperature:	-10°C to +55°C (+14°F to +130°F)
Supervised Points	
On-board Hardwire:	8 • Single or dual end-of-line (EOL) tamper point support • Point 1 supports two-wire smoke detectors • All points support four-wire smoke detectors • Enclosure tamper input (does not reduce point capacity)
Programmable Outputs (PO)	
On-board:	4 • **PO 1 only:** Configurable relay • **PO 2 to PO 4:** Configurable solid state • **PO 4 only:** Internal supervised speaker driver option
PO 1 Relay Rating:	• **Contacts:** 2 A with no jumper installed; resistive loads only • **Output:** 1.2 A with jumper installed; resistive loads only • **Operating Voltage:** 30 VDC maximum
PO 2 to PO 4 Rating:	400 mA current sink
Control Center	
Dimensions (H x W x D):	12 cm x 17.7 cm x 2.5 cm (4.7 in. x 7 in. x 1 in.)
Total Number Supported:	4
Recommended Mounting Surface:	Non-metallic surface
Minimum Mounting Distance:	1.2 m (4 ft) between each control center
Current Draw:	110 mA standby; 165 mA alarm
Minimum Wire Length:	3 m (10 ft)
Maximum Wire Length:	Total: 400 m (1312 ft) using using 0.8 mm (#22 AWG) wire; Single run: 100 m (328 ft) using 0.8 mm (#22 AWG) wire
Data Bus Wire Type Options:	• 1 four-conductor, power-limited 1.2 mm (#18 AWG) or 0.8 mm (#22 AWG) wire • At least 0.6 mm (#24 AWG) twisted pair CAT5 wire UL installations require power-limited wiring.
Audio Bus Wire Type Options:	• 1 two-conductor or 1 four-conductor, power-limited 1.2 mm (#18 AWG) or 0.8 mm (#22 AWG) wire. Only two conductors are used. • At least 0.6 mm (#24 AWG) twisted pair CAT5 wire UL installations require power-limited wiring. Unless using CAT5 cable, audio bus connections require a dedicated wire.
CAT5 Wire Requirements:	Refer to *Section 2.3 Control Center* Installation on page 10.
Number of…	
Users:	22 • **User 1:** Master user • **Users 2 to 21:** System users • **User 22:** Duress user
Events:	500 history events, stamped with time and date
Tokens and Key Fobs:	One per user (User 22 does not receive a token or key fob)

Phone Line	
Phone line trouble voltage:	Trouble condition occurs when the phone line voltage is between 1.10 V and 4.75 V
Control Panel Power Requirements	
AC Input Line Voltage	Use a UL Listed 18 V Class 2 transformer (22 VAC, VA 50/60 Hz), or the EZPS Power Supply (not investigated by UL).
Total Alarm Power:	1.4 A (AC power and standby battery; intrusion applications only). With a 7.0 Ah battery, the following current draws apply to all outputs and devices connected to the system: • Up to 170 mA for 24 hr for fire and combined fire/burglary applications • Up to 400 mA for 4 hr for UL burglary applications • Up to 1.2 A for other applications (not investigated by UL)
Auxiliary Power:	12 VDC, 1.0 A maximum. Includes 110 mA for each control center connected to the system, and up to 400 mA for the programmable outputs.
Current Draw:	85 mA standby; 160 mA alarm with all outputs activated
Voltage:	12 VDC nominal (11.2 VDC to 12.3 VDC) The control panel stops processing point faults when the voltage drops below 9.5 VDC.
Battery:	• D126 (7 Ah) or D1218 (18 Ah) sealed, lead acid rechargeable • 1.7 A maximum recharging current • Low battery condition occurs when battery drops below 12 VDC • If AC power fails and the battery drops below 9.5 VDC, the control panel stops processing point faults. Disconnect the battery under these conditions. • Maximum auxiliary current to recharge standby battery within 72 hours: - **12 V, 7 Ah Battery:** 400 mA - **12 V, 18 Ah Battery:** 900 mA
EZPS Power Supply Requirements (not investigated by UL)	
AC Input:	• **AC Input Voltage:** 100 VAC to 240 VAC • **Line Voltage Frequency:** 47 Hz to 63 Hz • **Maximum Input Current:** 0.5 A • **Power Factor:** Approximately 0.65 at full load
DC Output:	• **Nominal Output Voltage under AC line input:** 18 VDC • **Output Voltage Range under AC line input:** 16 VDC to 20 VDC • **Continuous Rated Output Current:** 1.25 A • **Output Current Limit:** Approximately 1.75 A to 2.5 A • **Periodic and Random Deviation (PARD):** Less than 250 mV
DX2010 Input Expander	
Operating Voltage:	8 VDC to 14 VDC
Current Draw:	35 mA standby; 135 mA maximum with connected accessories
Outputs:	100 mA, 12 VDC supervised output for accessories
Sensor Loop Terminal Wire Size:	0.8 mm (#22 AWG) to 1.8 mm (#14 AWG)
Wire Length:	• **Control panel to DX2010 (DX2010 auxiliary output not used):** - 0.8 mm (#22 AWG) = 305 m (1000 ft) - 1.2 mm (#1.2 mm) = 610 m (2000 ft) • **Control panel to DX2010 (DX2010 auxiliary output supplying 100 mA):** - 0.8 mm (#22 AWG) = 30 m (100 ft) - 1.2 mm (#1.2 mm) = 76 m (250 ft)
Operating Temperature:	+0°C to +50°C (+32°F to +122°F)
Relative Humidity:	5% to 85% @ +30°C (+86°F)
Sensor Loop Resistance:	60 Ω maximum
Sensor Loop:	Up to eight inputs; input contacts can be normally open (NO) or normally closed (NC) with appropriate EOL resistors for supervision.

Wireless Hub (ISW-BHB1-WX)	
Wire Gauge:	0.14 mm (#18 AWG) to 1.5 mm (#24 AWG)
Power/Voltage:	12 VDC nominal, 7 to 14 VDC
Wire Length:	100 m (328 ft)
Compliance:	EN50131-1 Security Grade 2 Type C, Environmental Class II

7.9 Compatible Options

Model Number	Description	Documentation Reference
C900V2	Conettix IP Dialer Capture Module Links the digital dialer to the Public Switched Telephone Network (PSTN), the digital dialer's telephone interface, and an Ethernet network.	F01U003472
CX4010	Plug-in Transformer For use in North America. 110 VAC primary voltage input. 18 VAC, 22 VA secondary input.	N/A
D132A	Smoke Detector Reversing Relay Module Allows the control panel to sound all smoke detectors connected to Point 1 when one smoke detector on the loop goes into alarm.	35567
DX2010	Input Expander Provides hard-wired expansion for an additional eight input points.	49533
ICP-EZPK	Programming Key Blue key for transferring information to and from Easy Series Intrusion Control Panels.	F01U004832
ICP-EZPS*	Wire-in Power Supply For use in Europe, the Middle East, Asia Pacific, Central and South America. 100 VAC to 240 VAC primary voltage input (AC).	F01U003732
ICP-EZPS-FRA*	AFNOR Power Supply For use in France. Provides 14 VDC and isolated auxiliary power outputs.	F01U008729
ICP-EZRU2	ROM Update Key Green key for performing Flash upgrades.	F01U025887
ICP-EZTS	Dual Tamper Switch Combination tamper switch with a wire loop for additional tamper outputs.	F01U003734
ICP-TR1822-CAN	Plug-in Transformer For use in Canada. 110 VAC primary voltage input. 18 VAC, 22 VA secondary input.	N/A
ISW-BHB1-WX*	wLSN Hub Provides wireless expansion for up to 32 input points. It is the interface to wLSN devices.	F01U009440
ITS-300GSM*	GSM Network Communicator Enables backup transmission from a control panel's telephone dialer over the GSM network if telephone transmission is not working. Transmits reports and audio.	F01U027641
IUI-EZ1	Oval Control Center Includes a speaker, microphone, function buttons, and a bubble level.	F01U003737
IUI-EZT-5	Easy Series Token Package Five Easy Series proximity tokens.	N/A
RPS-INTL*	Remote Programming Software Account management and control panel programming utility.	4998141259
TF008*	Plug-in Transformer For use in Australia and New Zealand. 240 VAC primary voltage input. 18 VAC, 1.3 A secondary input.	N/A

* Not investigated by UL.

Index

P

Q

R

S

T

U

V

W

Bosch Security Systems, Inc.
www.boschsecurity.com

F01U025147-01

BOSCH