Honeywell

VISTA-128BPT/VISTA-250BPT/ VISTA-128BPTSIA

Commercial Burglary Partitioned Security System With Scheduling

Installation and Setup Guide

800-06903 6/10 Rev A

Table of Contents

List of Figures

Conventions Used in This Manual

Before you begin using this manual, it is important that you understand the meaning of the following symbols (icons).

UL These notes include specific information that must be followed if you are installing this system for a UL Listed application.

These notes include information that you should be aware of before continuing with the installation, and that, if not observed, could result in operational difficulties.

This symbol indicates a critical note that could seriously affect the operation of the system, or could cause damage to the system. Please read each warning carefully. This symbol also denotes warnings about physical harm to the user.

ZONE PROG?
1 = YES 0 = NO 0

Many system options are programmed in an interactive mode by responding to alpha keypad display prompts. These prompts are shown in a single-line box.

✶00 Additional system options are programmed via data fields, which are indicated by a "star" (✶) followed by the data field number.

PRODUCT MODEL NUMBERS:

Unless noted otherwise, references to specific model numbers represent Honeywell products.

SIA CP-01 Quick Reference Chart

The minimum required system for SIA CP-01 is a VISTA-128BPTSIA Control, 6160 Keypad and a UL Listed Bell.

Item	Feature	Range	Shipping Default	SIA Requirement*
*09	Entry Delay # 1	02 – 15 multiplied by 15 seconds 00 = 240 sec (4 minutes)	30 Seconds`	At least 30 Seconds **
*10	Exit Delay #1	03 – 15 multiplied by 15 seconds	60 Seconds	60 Seconds
*11	Entry Delay # 2	02 – 15 multiplied by 15 seconds 00 = 240 sec (4 minutes)	30 Seconds	At least 30 Seconds **
*12	Exit Delay #2	03 – 15 multiplied by 15 seconds	60 Seconds	60 Seconds
*28	Power Up in Previous State	0 = no 1 = yes	Yes	Yes
*57	Dynamic Signaling Priority	0 = primary dialer 1 = Communicator as first reporting destination	0 (primary dialer)	0 (primary dialer)
*84	Swinger Suppression	01-06 = 1–6 alarms	2 alarms	1 alarm
*88	Abort Window Time (for non-fire zones)	1 = 15 seconds 2 = 30 seconds 3 = 45 seconds	30 Seconds	At least 15 Seconds **
1*20	Exit Error	0 = no 1 = Bypass E/E and interior zones faulted after exit delay	1 (Enabled)	1 (Enabled)
1*21	Exit Time Reset	0 = no 1 = Resets Exit Delay to programmed value after zone is closed and then faulted prior to end of exit delay.	1 (Enabled)	1 (Enabled)
1*22 – 1*25	Cross Zoning	Zone 001 – 128 000, 000 = Disabled	Disabled	Enabled and two (or more) zones programmed
1*42	Call Waiting Defeat	0 = no 1 = yes	Disabled (0)	Enabled if user has call waiting
1*61	Abort Verify	0 = Disable 1 = Enable	Enabled	Enabled
Zone Programming Auto Stay Zone, Zone type 04 has this feature enabled by default	Auto Stay Arm or Occupied Premises	0 = Disable 1 = Enable	1 (Enabled)	Enabled

Item	Feature	Range	Shipping Default	SIA Requirement*
Zone Programming (Abort Window Enable)	Abort Window (for non-fire zones)	0 = no abort window 1 = yes, use abort window according to *88 selection	1 = yes	Yes (all non-fire zones)
Zone Programming (Swinger Suppression Enable)	Swinger Suppression Enable	0 = no suppression 1 = yes, suppress alarms according to *84 selection	Yes (enabled)	Yes (enabled (all zones))
Zone Programming Tamper Option	Fire Alarm Verification	For Zone Response Type 16 (Fire) tamper selection must be set to "0"	Disabled	Enabled unless sensors can self verify
-	Exit Time and Progress Annunciation/Disable for Remote Arm (Not Evaluated for SIA CP-01)	Always Enabled	Enabled	Enabled
-	Programmable Cross Zoning Time	Both zones must be faulted within 5 minutes	Per Manufacturer	Per walk path in protected premises
-	Cancel Window	5 minutes	Enabled	Not required to be programmable
-	Cancel Annunciation - Keypad displays "Alarm Cancel" when report is received	NA	Enabled	Enabled
User Authority Level 6	Duress Feature	NA	Disabled	Disabled

* Programming at installation may be subordinate to other UL requirements for the intended application.

** Combined Entry Delay and Abort Window should not exceed 1 minute.

NOTES:

- Using the Call Waiting Cancel feature on a non-Call Waiting line will prevent successful communication to the central station.
- The control unit must be installed with a local sounding device and an off-premise transmission for Contact ID communication format.
- Refer to the User Guide for procedures on Testing the System.
- During Test mode, no alarm reports are sent to the central monitoring station.

General Description

About the VISTA-128BPT/VISTA-250BPT

All references to the VISTA-128BPT also pertain to the VISTA-128BPTSIA. The differences between the two panels are outlined in the SIA CP-01 Quick Reference Chart located at the beginning of this manual.

The VISTA-128BPT/VISTA-250BPT is an 8-partition, UL Listed control panel with the following features:

- Supports hardwired, polling loop, and wireless zones
- Supervision of bells, keypads, RF receivers, and output devices
- Scheduling capabilities (allows certain operations to be automated)

The VISTA-128BPT/VISTA-250BPT can interface with the following devices:

- Graphic/Touch-Screen Keypads

UL Graphic Keypads (AUI, GUI) are not Listed for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

- Voice Keypad (6160V)

UL Voice Keypad 6160V cannot be used for SIA Installations.

- An ECP Communication Device that can send Contact ID messages
- An access control system by using the ADEMCO VistaKey module (via the polling loop)

UL The access control function is not Listed for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

NOTE: All references in this manual for number of zones, number of user codes, number of access cards, and the event log capacity, use the VISTA-250BPT's features. The following table lists the differences between the VISTA-128BPT and the VISTA-250BPT control panels. All other features are identical.

Feature	VISTA-128BPT	VISTA-250BPT
Number of Zones	128	250
Number of User Codes	150	250
Number of Access Cards	250	500
Event Log Capacity	512	1000
VistaKey Modules	8	15

Features

Hardwire and Optional Expansion Zones

- Provides nine hardwire zones.
- Supports up to 16 2-wire smoke detectors on zone 1.
- Automatically resets 4-wire smoke detectors using the J7 output when a code + off is entered.
- Triggers the built-in sounders on other hardwired smoke detectors if one smoke detector annunciates an alarm. This feature requires a 4204 Relay Module.
- Provides tamper supervision on the hardwire zones.
- Supports up to 241 additional expansion zones (119 for the VISTA-128BPT) using a built-in polling (multiplex) loop.
- Supports up to 249 wireless zones (127 for the VISTA-128BPT) (fewer if using hardwire and/or polling loop zones).

UL The 5881ENHC RF Receiver, 5869 Holdup Switch Transmitter and 5817CB Wireless Commercial Household Transmitter are listed for UL Commercial Burglary applications. All other RF receivers and transmitters are not listed for UL Commercial Burglary applications.

ULC Wireless devices are not ULC Listed and cannot be used for ULC Installations.

- Can program burglary zones as silent in the alarm condition (alarm output is silent and the keypad does not display or sound the alarm).
- Provides three keypad panic keys: 1 + ✳ (A), ✳ + # (B), and 3 + # (C).
- Remote Interactive Service (RIS) allows access to the 7845i-ent Communicator from a wireless phone or web browser.

UL Use of Remote Interactive Services is not permitted in UL installations.

- Anti-Mask is used if a zone type 04 (interior) or 10 (interior with delay) and input type 06 (serial poll) are selected. The trouble report code is used to report the masking.

UL The Anti-Mask feature is not permitted in UL installations.

- A Smart contact option that may be selected for devices that support this feature such as the 5193SDT Smoke Detector or PIRs.
- Battery sensing hardware that can sense when the battery voltage is too low and prevents deep discharging from not occurring.

Peripherals Devices

- Supports up to 31 addressable devices, (keypads, RF receivers, relay modules, etc.).
- Supervises devices (keypads, RF receivers, and relay modules) and individual relays (up to 32), as well as system zones (RF receivers and keypad panics).
- Provides 96 outputs using 4204 Relay Modules, V-Plex Relay Modules and X-10 devices can activate outputs in response to system events (alarm condition), at a specific time of day, at random times, and manually using the #70 Relay Command Mode.
- Supports the ADEMCO 4286 VIP Module, which allows access to the system from either a remote location or on the premises

UL The VIP Module is not Listed for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

- Supports the ADEMCO 4146 Keyswitch on any one of the system's eight partitions.

Arming/Disarming and Bypassing

- Can arm the system with zones faulted (Vent Zone). These zones are automatically bypassed and can be programmed to automatically unbypass when the zone restores.
- Can arm with entry/exit and interior type zones faulted (Arm w/Fault). These zones must be restored before the exit delay expires, otherwise an alarm is generated.

UL
- Vent zones cannot be used in UL installations.
- You **must disable** the Force Arm option (used in conjunction with the Arm w/Fault option), in UL installations.

ULC You **must disable** the Force Arm option (used in conjunction with the Arm w/Fault option), in ULC Installations.

- Provides global arming capability (ability to arm all partitions the user code has access to in one command).
- Can Quick Exit an armed premises without having to disarm and then rearm the system.

UL Quick Exit is not permitted for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

- Can be armed in one of three STAY modes or Instant modes, automatically bypassing specific burglary zones regardless of the zone response type.
- Can automatically bypass specific zones if no one exits the premises after arming (Auto-STAY). Auto-STAY will not occur if the system is armed via an RF transmitter, VIP module, scheduling, access control, keyswitch, RS232 (TB4) automation or downloading.
- Can bypass a group of zones with one set of keystrokes.
- Supports Exit Error Logic, whereby the system can tell the difference between a regular alarm and an alarm caused by leaving an entry/exit door open. If the system is not subsequently disarmed, faulted E/E zone(s) and/or interior zones are bypassed and the system arms.
- Supports Recent Close report, which is designed to notify the central station that an alarm has occurred within 2 minutes after the exit delay has expired.

Partitioning

- Can control eight separate areas independently, each functioning as if it had its own separate control.
- Provides a Common Lobby partition, which can be programmed to arm automatically when the last partition is armed, and to disarm when the first partition is disarmed.
- Provides a Master partition (9), used for the purpose of viewing the status of all partitions at the same time.
- Can display fire, burglary, panic, and trouble conditions at all other partitions' keypads (selectable option).

Scheduling

ULC Scheduling cannot be used for ULC Installations.

- Can automate system functions, such as arming, disarming, and activation of outputs (e.g., lights).
- Provides access schedules (for limiting system access to users by time).
- Provides an End User Output Programming Mode, allowing the user to control outputs.

Access Control

- Supports up to 15 VistaKey modules (15 access points) (VISTA-128BPT supports 8 modules), which are used for access control. It is a single-door access control module.
- Support up to 500 access cards (250 in VISTA-128BPT).
- Can store access control events in the event log.

System Communication

- Supports ADEMCO Contact ID; ADEMCO 10-Digit Contact ID and 4+2 Express formats.

The system is shipped defaulted for Contact ID communication. It is the only format capable of uniquely reporting all 250 zones, as well as openings and closings for all 250 users. This requires central stations to be equipped with the MX8000 receiver or equivalent to fully support all new VISTA-128BPT/VISTA-250BPT report codes. If you need to update your MX8000 receiver, contact your distributor.

- Supports Dynamic Signaling feature, which prevents redundant signals being sent to the central station when both the built-in dialer and Communication Devices are used.
- Provides the Dialer Queue Report in the event of a loss of communications between the dialer and the central station, i.e. telco loss. The total events that will be queued up are 128 (91 Burg + 37 Life Safety). A Dialer Queue Overflow report (E354) will be sent if the report queue goes beyond its limits. Note that: Life Safety includes Fire, CO, 24 HR Silent/Audible/Auxiliary, and Duress. Life Safety events may go beyond 37 (up to 128) if there are no Burg events in the queue. If all dialer attempts are exhausted before communication to the central station is restored, the queue will be cleared.

Downloading

- Supports upload and download capability.
- Can periodically and automatically perform a scheduled download.
- Can be downloaded via the following 7845i-ent, 7845GSM or 7845i-GSM using Compass revision 1.5.8 or above.

UL Unattended and Scheduled Downloading are not UL Listed features.

- Can download access control cardholder information.

Event Log

- Provides an event log (history log) that can store up to 1000 events (512 for VISTA-128BPT).
- Can view the event log on an alpha or graphic/touch-screen keypad.

Additional Features

- Provides up to 60 installer-defined, custom words that can be used for zone descriptors.
- Provides 32 keypad macro commands (each macro is a series of keypad commands of up to 32 keystrokes) using the A, B, C, and D keys by partition.
- Provides cross-zone capability, which helps prevent false alarms by preventing a zone from going into alarm unless its cross-zone is also faulted within a 5-minute period.
- Contains a built-in User Manual, which provides the end user with a brief explanation of the function of a key when the user presses any of the function keys on the keypad for 5 seconds.
- Provides an RS232 input (TB4) for serial data. This is useful for interfacing the system with Automation software. Automation software cannot be used if a serial printer is used on the system.

At least one 2-line alpha keypad (6160) must be connected to the system for programming (if you are using keypad programming), and must remain connected to the system in order to allow the primary user to program additional user codes into the system at a later time.

Partitioning

Theory of Partitioning

This system provides the ability to arm and disarm up to eight different areas, as if each had its own control. These areas are called partitions. A Partitioned system allows the user to disarm certain areas while leaving other areas armed, or to limit access to certain areas to specific individuals. Each system user can be assigned to operate any or all partitions, and can be given a different authority level in each.

Before anything can be assigned to those partitions, you must first determine how many partitions (1-8) are required. Following are some facts you need to know about partitioning.

Keypads

Each keypad must be given a unique "address" and be assigned to one partition. It can also be assigned to Partition 9 if Master keypad operation is desired. (See "Master Keypad Setup and Operation" later in this section.)

Zones

Each zone must be assigned to one partition. The zones assigned to a partition will be displayed on that partition's keypad(s).

Users

Each user may be given access to one or more partitions. If a user is to operate more than one partition and would like to arm/disarm all or some of those partitions with a single command, the user must be enabled for Global Arming for those partitions (when entering user codes).

A user with access to more than one partition (multiple access) can "log on" to one partition from another partition's keypad, provided that program field 2*18: Enable GOTO is enabled for each partition he/she wants to log on to from another.

A partition can be selected as a "common lobby" partition, and other partitions can affect this partition by causing arming/disarming of this partition to be automated (see "Common Lobby Logic" later in this section).

Setting-Up a Partitioned System

The basic steps to setting up a partitioned system are described below. If you need more information on how to program the options, see *SECTION 4: Programming*.

1. Determine how many partitions the system will consist of (programmed in field 2*00).
2. Assign keypads to partitions (*Device Programming* in the #*93 Menu Mode*).
3. Assign zones to partitions (*Zone Programming* in the #*93 Menu Mode*).
4. Confirm zones are displayed at the keypad(s) assigned to those partitions.
5. Assign users to partitions.
6. Enable the GOTO feature (program field 2*18) for each partition a multiple-access user can log on to (alpha keypad only).
7. Program partition-specific fields (see the *Data Field Descriptions* section).

Common Lobby Logic

When an installation consists of a partition shared by users of other partitions in a building, that shared partition may be assigned as the "common lobby" partition for the system (program field 1*17). An example of this might be in a medical building where there are two doctors' offices and a common entrance area (see example that follows explanation).

The Common Lobby feature employs logic for automatic arming and disarming of the common lobby. Two programming fields determine the way the common lobby will react relative to the status of other partitions. They are: 1*18 Affects Lobby and 1*19 Arms Lobby.

1*18 Affects Lobby (must be programmed by partition)

Setting this field to 1 for a specific partition causes that partition to affect the operation of the common lobby as follows:

a. When the first partition that affects the lobby is disarmed, the lobby is automatically disarmed.

b. The common lobby cannot be armed unless every partition selected to affect the lobby is armed.

1*19 Arms Lobby (must be programmed by partition)

Setting this field to 1 for a specific partition causes that partition to affect the operation of the common lobby as follows:

a. The common lobby cannot be armed unless every partition selected to affect the lobby is armed.

b. Arming a partition that is programmed to arm the lobby causes the system to automatically attempt to arm the lobby. If any faults exist in the lobby partition, or if another partition that affects the lobby is disarmed, the lobby cannot be armed, and the message "UNABLE TO ARM LOBBY PARTITION" is displayed.

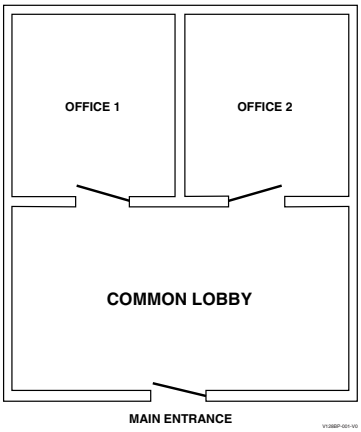
You cannot select a partition to "arm" the lobby unless it has first been selected to "affect" the lobby. Do not enable field 1*19 without enabling field 1*18.

The following chart sums up how the common lobby partition will operate.

1*18 Affects Lobby	1*19 Arms Lobby	Disarms when partition disarms?	Attempts to arm when partition arms?	Can be armed if other partitions disarmed?
0	0	NO	NO	YES
1	0	YES	NO	NO
1	1	YES	YES	NO
0	1	---ENTRY NOT ALLOWED---		

Example

Here is an example of how the lobby would react in a typical setup.



User #1 has access to Office #1 and the Common Lobby.

User #2 has access to Office #2 and the Common Lobby.

Office #1 is set up to affect the Common Lobby, but not arm it.

Office #2 is set up to affect and arm the Common Lobby.

NOTE: In the tables below, the notations in parentheses ( ) indicate the current status of the other partition when the user takes action.

Sequence #1:

	Office 1	Office 2	Lobby Action
User #1:	Disarms	(Armed)	Disarms
User #2:	(Disarmed)	Disarms	No Change
User #1:	Arms	(Disarmed)	No change
User #2:	(Armed)	Arms	Arms

Sequence #2:

	Office 1	Office 2	Lobby Action
User #2:	(Armed)	Disarms	Disarms
User #1:	Disarms	(Disarmed)	(No change)
User #2:	(Disarmed)	Arms	No Change
User #1:	Arms	(Armed)	No Change

Notice that in sequence #1, because Office #2 was the last to arm, the lobby also armed (Office #2 is programmed to affect and arm the lobby). In sequence #2, the lobby could not arm when Office #2 armed, because Office #1, which affects the lobby, was still disarmed.

When Office #1 armed, the lobby still did not arm because Office #1 was not programmed to arm the lobby. User #1 would have to arm the lobby manually. Therefore, you would want to program a partition to affect and arm the lobby if the users of that partition are expected to be the last to leave the building.

How User Access Codes Affect the Common Lobby

Codes with Global Arming

If a code is given "global arming" when it is defined (see *SECTION 9: User Access Codes*), the keypad prompts the user to select the partitions they want to arm. Only the partitions the user has access to are displayed. This allows the user to choose the partitions to be armed or disarmed, and so eliminates the "automatic" operation of the lobby. Keep in mind, however, that if a user attempts to arm all, and another "affecting" partition is disarmed, the user cannot arm the lobby, and the message "UNABLE TO ARM LOBBY PARTITION" is displayed.

Codes with Non-Global Arming

If a user arms with a non-global code, the lobby partition operation is automatic, as described by fields 1*18 and 1*19.

Other Methods of Arming/Disarming

Common Lobby logic remains active when arming or disarming a partition that affects and/or arms the common lobby in one of the following manners:

- Quick-Arm
- Keyswitch
- Wireless Button
- Wireless Keypad

Arming/Disarming Remotely

If a user arms or disarms remotely (through Compass downloading software), the lobby does not automatically follow another partition that is programmed to arm or disarm the lobby. The lobby must be armed separately, after arming all affecting partitions first.

Auto-Arming/Disarming

If scheduling is used to automatically arm and/or disarm partitions, the common lobby partition does not automatically follow another partition that is programmed to arm or disarm the lobby.

The lobby must be included as a partition to be armed/disarmed and must be scheduled as the last partition armed.

If you are using auto-arming, make sure that the **Auto-Arm Delay** and **Auto-Arm Warning** periods, for the lobby partition, (fields 2*05 and 2*06) combined are longer than that of any other partition that affects the lobby. This causes the lobby to arm last.

Master Keypad Setup and Operation

Although this system has eight actual partitions, it provides an extra partition strictly for the purpose of assigning keypads as Master keypads for the system.

Assigning any keypad to Partition 9 in *Device Programming* in the *#93 Menu Mode* makes that keypad a Master keypad. A Master keypad reflects the status of the entire system (Partitions 1-8) on its display at one time. This is useful because it eliminates the need for a building security officer to have to log on to various partitions from one partition's keypad to find out where an alarm has occurred.

The following is a typical display:

```
SYSTEM  12345678
STATUS  RRNNA TB
```

Possible status indications include:

A = Armed Away **S** = Armed Stay **M** = Armed Maximum
C = Comm Fail **I** = Armed Instant **R** = Ready
N = Not Ready **B** = Bypassed/Ready ✳ = Alarm
T = Trouble **F** = Fire Alarm **P** = AC Power Failure
L = Low System Battery

To obtain more information regarding a particular partition, enter [✳] + Partition No. (e.g., [✳] + [4]). This allows viewing only of that partition. In order to affect that partition, the user must use a code that has access to that partition.

Also, in order for a user of any partition to log on to Partition 9 to view the status of all partitions, that user must have access to all partitions. Otherwise, access is denied.

The following is displayed for a fault condition on Zone 2 (Loading Dock Window) on Partition 1 (Warehouse) when a user logs on from a keypad on Partition 9:

```
WHSE  DISARMED
HIT T FOR FAULTS
```

Pressing [✳] causes the following display to appear at Partition 1's keypad(s):

```
FAULT 002  LOADING
DOCK  WINDOW
```

Additional zone faults are displayed one at a time. To display a new partition's status, press [✳] + Partition No.

The Armed LED on a Master keypad is lit only if all partitions have been armed successfully. The Ready LED is lit only if all partitions are "ready to arm." The Ready LED is lit if only one partition is armed. Neither LED is lit if only some partitions are armed and/or only some partitions are ready.

Press [✳] + [0] or [✳] + [9] to return to the master partition. Otherwise, if no keys are pressed for 2 minutes, the system automatically returns to the master partition

The sounder on a Master keypad reflects the sound of the most critical condition on all of the partitions. The priority of the sounds, from most to least critical, is as follows:

1. Pulsing fire alarm sounds
2. T4 CO alarm sounds
3. Steady burglar alarm sounds

4. Trouble sounds (rapid beeping)

Silence the sounder by pressing any key on the Master keypad or a keypad on the partition where the condition exists.

A Master keypad uses the same panics as Partition 1. Master keypad panics are sent to Partition 1, and will activate on Partition 1. Therefore, panics must be programmed for Partition 1.

Installing the Control

This section describes the procedures for mounting and wiring the control panel and all the peripheral devices.

NOTE: All references in this manual for number of zones, number of user codes, number of access cards, and the event log capacity, use the VISTA-250BPT's features. See *SECTION 1: General Description* for the table listing the differences between the VISTA-128BPT and the VISTA-250BPT control panels.

Mounting the Control Cabinet

To mount the control cabinet, perform the following steps:

Step	Action
1	Before mounting the circuit board, remove the metal knockouts for the wiring entry that you will be using. **DO NOT ATTEMPT TO REMOVE THE KNOCKOUTS AFTER THE CIRCUIT BOARD HAS BEEN INSTALLED.**
2	Using fasteners or anchors (not supplied), mount the control cabinet to a sturdy wall in a clean, dry area that is not readily accessible to the general public. The back of the cabinet has 4 holes for this purpose.

UL To provide certificated burglary service for UL installations, refer to the special requirements and *Figure 3-2 Cabinet Attack Resistance Considerations* to follow. For UL Commercial Burglary installations that require ATTACK RESISTANCE, use the cabinet included in the COM-UL Commercial Enclosure.

Installing the Cabinet Lock

1. Remove cabinet door, then remove the lock knockout from the door. Insert the key into the lock.
2. Position the lock in the hole, making certain that the latch will make contact with the latch bracket when the door is closed.
3. When correctly positioned, insert supplied lock clip on the inside of the cabinet into the slots on the lock cylinder. Use ADEMCO Lock # N6277V1 and Lock Clip # P3422-2 (supplied).

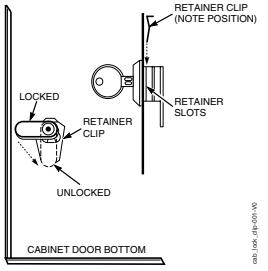


Figure 3-1: Installing the Lock

Mercantile Premises Listing Guidelines

- The panel door must be supervised. Mount the clip-on tamper switch (supplied) to the cabinet's right side wall as shown in the diagram below, and wire it to one of the hardwire zones.
- Use a bell with a tamper-protected housing such as the ADEMCO AB12M. The bell housing's tamper switch and inner tamper linings must also be wired to the hardwire zone.
- Assign the tampers' hardwire zone to a burglary partition. Program the hardwire zone for day trouble/night alarm (zone type 5) when only one burglary partition is used. Program it for 24-hr. audible alarm (zone type 7) when more than one burglary partition is used.

ULC 24-Hour audible alarm (Zone types 6 and 7) is not approved for ULC application.

- All wiring between the bell and panel must be run in conduit. Remaining wires do not need to be run in conduit.
- All wiring that is not run in conduit must exit from the knockout openings on the bottom or back of the cabinet.

- All unused knockouts must be plugged using the disc plugs and carriage bolts (supplied), as indicated in the diagram below.
- Fasten the cabinet door to the cabinet backbox using the 18 one-inch-long Phillips-head screws (supplied) after all wiring, programming, and checkout procedures have been completed.

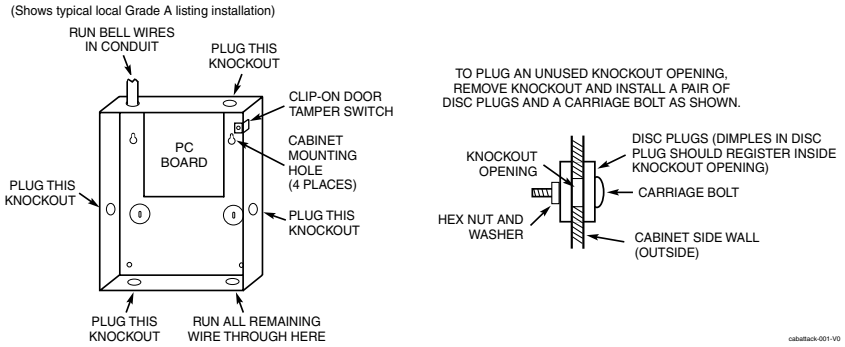


Figure 3-2: Cabinet Attack Resistance Considerations

Mercantile Safe and Vault Listing Guidelines

- Follow the guidelines given above for Mercantile Premises listing.
- Mount a shock sensor such as Sentrol No. 5402 to the control's backbox. Follow the manufacturer's instructions for proper sensor mounting. This sensor also must be wired to a hardwire zone.
- For safe and vault applications, a UL Listed contact must be used inside the cabinet through one of the knockouts for pry-off tamper purposes. This sensor also must be wired to a hardwire zone.

Installing the Control's Circuit Board

To install the circuit board in the cabinet, perform the following steps:

Step	Action
1	Hang the three mounting clips on the raised cabinet tabs. Refer to *Figure 3-3* (Detail B). Make sure the clip orientation is exactly as shown in the diagram to avoid damage. This will also avoid problems with insertion and removal of the PC board.
2	Insert the top of the circuit board into the slots at the top of the cabinet. Make certain that the board rests in the slots as indicated (Detail A).
3	Swing the base of the board into the mounting clips and secure the board to the cabinet with the accompanying screws.

NOTES:

- Make certain that the mounting screws are tight. This ensures that there is a good ground connection between the PC board and the cabinet.
- Dress field wiring away from the microprocessor (center) section of the PC board. Use the loops on the left and right sidewalls of the cabinet for anchoring field wiring using tie wraps (Detail C). These steps are important to minimize the risk of panel RF interference with television reception.

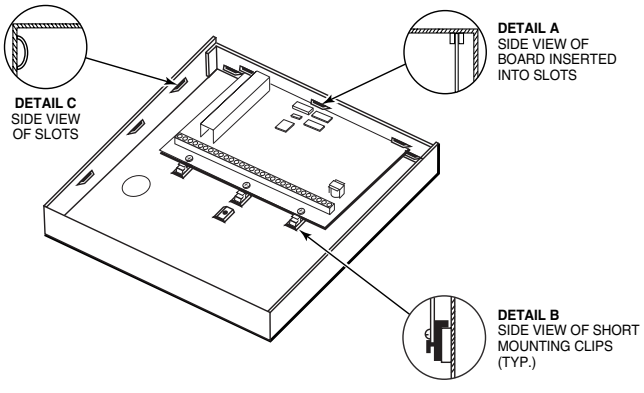


Figure 3-3: Mounting the PC Board

Installing the Keypads

Up to 31 addressable keypads (addresses 00-30) may be used (you may need to use an auxiliary power supply if the 750mA aux. output is exceeded).

NOTE: Refer to the Alpha Vocabulary list found in the *#93 Menu Mode* in the *Programming Guide* for list of the words annunciated by the 6160V.

NOTE: The 6160V keypad is not to be used in SIA installations.

To wire the keypads, perform the following steps:

Step	Action
1	Determine wire gauge by referring to the Wire Run Length/Gauge table below.
2	Wire keypads to a single wire run or connect individual keypads to separate wire runs. The maximum wire run length from the control to a keypad, which is homerun back to the control must not exceed the lengths listed in the table.
3	Run field wiring from the control to the keypads (using standard 4-conductor cable of the wire gauge determined in step 1).
4	Connect the keypad(s) to terminals 6, 7, 8, and 9 on the control board, as shown in *Figure 3-4*.

Wire Run Length/Gauge Table

Wire Gauge	Length
#22 gauge	450 feet
#20 gauge	700 feet
#18 gauge	1100 feet
#16 gauge	1750 feet

- The length of all wire runs combined, regardless of the wire gauge, must not exceed 2000 feet when unshielded quad conductor cable is used (1000 feet if unshielded cable is run in conduit, which acts a shield, or if shielded cable is used).
- If more than one keypad is wired to one run, then the above maximum lengths must be divided by the number of keypads on the run (e.g., the maximum length is 225 feet if two keypads are wired on a #22 gauge run).

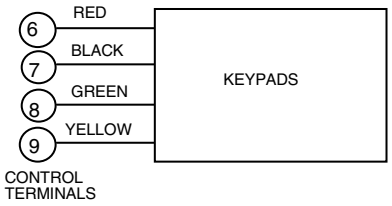


Figure 3-4: Keypad Connections to Control Panel

Addressing the Keypads

The keypads will not operate until they are physically addressed and enabled in the system's *Device Programming* in the *#93 Menu Mode*.

Set each keypad for an individual address (00-30) according to the keypad's instructions. Set an alpha keypad for address 00 and other keypads for higher addresses (00 and 01 are enabled in the system's default program). Any keypads set for address 02 and above will appear blank until they are enabled in the system's program. Each keypad must be set for a different address.

- Do not set any keypads to address 31 (nonaddressable mode). They will interfere with other keypads (as well as other devices) connected to the keypad terminals.
- If an "OC" or "OPEN CIRCUIT" message is present on a keypad, data from the control is not reaching the keypad. Check your wiring.

Supplementary Power Supply for Additional Keypads

When the control's auxiliary power load for all devices exceeds 750mA, you can power additional keypads from a regulated 12VDC power supply (e.g., ADEMCO AD12612 (1.2A)). Use a UL Listed, battery-backed supply for UL installations.

Connect the additional keypads as shown in *Figure 3-5*, using the keypad wire colors shown. Be sure to observe the current ratings for the power supply used.

- Make connections directly to the screw terminals as shown in *Figure 3-5*. Make no connection to the blue wire (if present).
- Be sure to connect the negative (–) terminal on the power supply unit to terminal 7 (**–**) on the control.

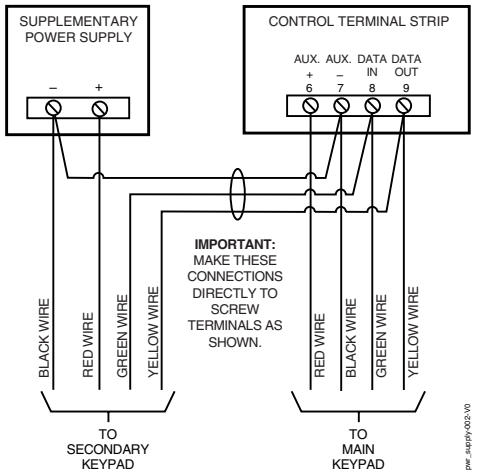


Figure 3-5: Using a Supplementary Power Supply

Installing External Sounders

The VISTA-128BPT/VISTA-250BPT provides a bell circuit output for operating fire and burglary alarm notification appliances. The alarm output is rated as follows: 10VDC – 14VDC, 1.7A max., power-limited.

UL

- For Household Fire and combination Household Fire/Burglary installations, the total current drawn from the auxiliary power, polling loop, and alarm output combined must not exceed 750mA.
- For Household Burglary installations, the total current drawn from the alarm output must not exceed 1.7A. A battery must be installed, as it supplies the current for the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

The output has the following options:

- Selectable for supervision.
- Selectable for confirmation of arming ding.
- Selectable to chime when entry/exit or perimeter zones are faulted.
- Selectable for no timeout or timeout of 2-30 minutes.

UL Burglary bell circuits must be programmed for a timeout of 16 minutes or longer.

UL985 Household Fire or Combination Household Fire/Burglary Installations

For installations that must provide UL Listed protection, the total combined current drawn from the alarm output, auxiliary power output, and polling loop must not exceed 750mA in order to comply with the battery independence requirements.

UL1023 Household Burglary Installations

For Household Burglary installations, the total current drawn from the alarm output must not exceed 1.7A. A battery must be installed, as the battery supplies current from the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

Non-UL Installations

For non-UL installations, the total current drawn from this output can be up to 1.7A. A battery must be installed, as the battery supplies current in excess of 750mA. Up to two 719 sirens can be used wired in parallel.

UL This control complies with National Fire Protection Association (NFPA) requirements for temporal pulse sounding of fire notification appliances.

Alarm Output Supervision

When supervision is enabled, the VISTA-128BPT/VISTA-250BPT monitors the alarm output wiring for open and short circuit faults while the output is inactive. The system provides a trouble indication (Zone 970) when an open occurs; or when a short occurs between the Bell (+) and Bell (-) terminal wiring, or between the Bell (+) terminal wiring and earth ground.

UL **NOTE:** When supervising the bell output (zone 970), only one device can be connected to the alarm output (terminals 4 and 5) for UL and Fire installations.

The VISTA-128BPT/VISTA-250BPT indicates the trouble condition regardless of whether the system is armed or disarmed. The zone displays on the keypads, reports to the event log, and transmits to the central station (if programmed) on Partition 1. The Contact ID event code is 321, Bell Trouble. The trouble is cleared from the display by entering the user code + OFF.

Wiring the Alarm Output

The wiring of the alarm output depends upon whether you are going to supervise the output or not. Use the appropriate procedure below for your application.

UL Use only UL Listed sounding devices for UL installations.

Compatible Alarm Indicating Devices

Model Number	Device Type	Polarizing Diode
719	Compact Outdoor Siren(not UL Listed)	Yes
747	Indoor Siren	Yes
AB12M	Bell	Yes
System Sensor HR	Fire Piezo Horn	No
System Sensor P2RK, P4RK	Fire Horn/Strobe	No
Wheelock AS-121575W	Fire Horn/Strobe	No

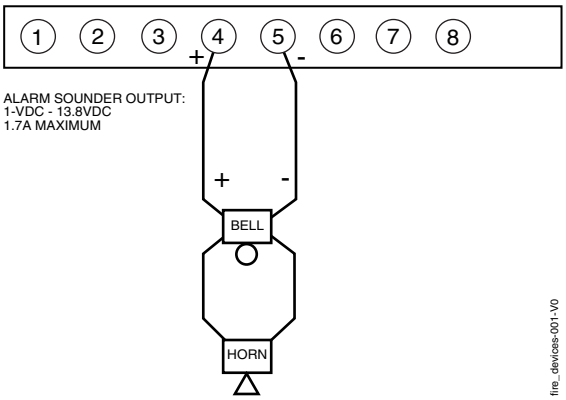


Figure 3-6: Wiring Polarized Fire Devices

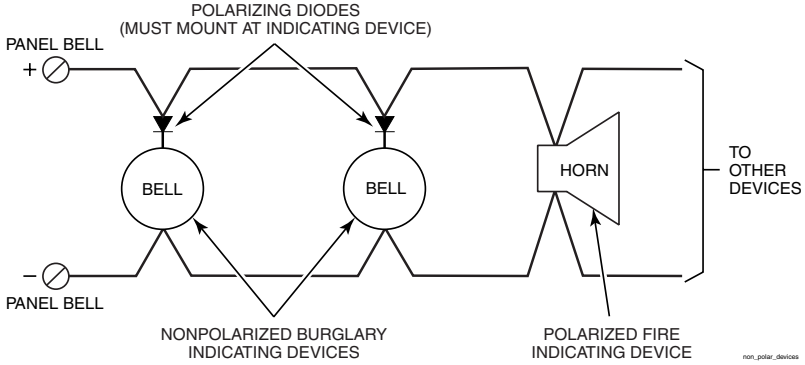


Figure 3-7: Wiring Nonpolarized Burglary Devices

Supervising the Alarm Output

To wire the alarm output using the supervision feature, perform the following steps:

Step	Action
1	Wire polarized fire-indicating devices to the alarm output as shown in *Figure 3-6*.
2	Wire nonpolarized burglary indicating devices to the alarm output using a polarizing diode (two 2A diodes supplied), as shown in *Figure 3-7*.
3	Program Zone 970 with a response type of 05 (trouble by day/alarm by night). **NOTE:** When supervising the bell output (zone 970), only one device can be connected to the alarm output (terminals 4 and 5) for UL and Fire installations.

The minimum load on the alarm output must exceed 5mA at 12V for proper supervision operation.

UL If a device such as a siren driver with a high-resistance trigger input (drawing less than 5mA) is used in a UL Household Fire installation, the siren driver must independently supervise siren speaker wiring.

Using a Siren Driver

To install a siren driver, perform the following steps:

Step	Action
1	Mount the siren driver in the panel's cabinet.
2	Wire the siren driver to the control and to the speaker(s). (See the driver's instructions.)
3	Cut the blue jumper on the upper left-hand corner of the panel's PC board.
4	Program Zone 970 with no response type (00).

Disabling the Supervision of the Alarm Output

To install the alarm output and disable the supervision feature, perform the following steps:

Step	Action
1	Wire the devices to terminals 4 and 5, observing polarity if necessary.
2	Cut the blue jumper on the upper left-hand corner of the panel's PC board.
3	Program Zone 970 with no response type (00).

Telephone Line Connections

Connect the main dialer output to telephone company lines using the RJ31X cables supplied.

UL The telephone line inputs have overvoltage protection in accordance with UL1459, as specified in UL985/UL1023.

The system is shipped defaulted for Contact ID format. It is the only format capable of uniquely reporting all 250 zones, as well as openings and closings for all 250 users. This requires central stations to be equipped with the Honeywell MX8000 receiver or equivalent. If you need an update, contact your distributor.

To prevent the risk of shock, disconnect phone lines at the telco jack before servicing.

If the communicator is connected to a PABX, be sure it has a backup power supply that can support the PABX for 24 hours (central station) or 60 hours (remote station). Many PABXs are *not* power-backed up, and this can result in a communication failure if power is lost.

Reporting Formats

The system supports the following formats:

ADEMCO Contact ID; ADEMCO 10-Digit Contact ID and 4 + 2 Express.

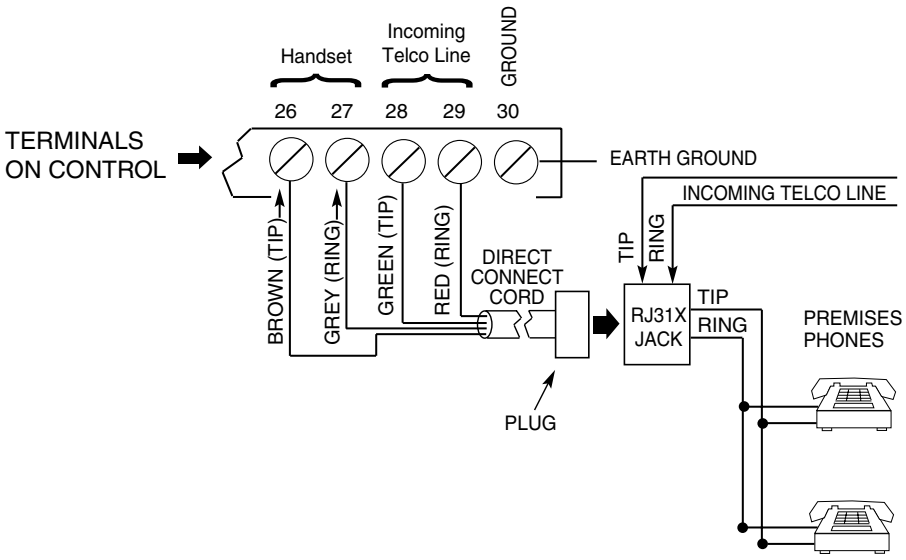


Figure 3-8: Telephone Line Connections

Wiring Burglary, Panic and Smoke Detector Devices to Zones 1-9

The maximum zone resistance is 100 ohms for zones 1 and 8, and 300 ohms for all other zones (excluding the 2K EOL resistor).

ULC Smoke detector devices have not been evaluated for ULC installations.

To wire burglary and panic devices to zones 1-9, connect sensors/contacts to the hardwire zone terminals (10 through 23). See *Figure 3-9*. Connect N.C. and N.O. devices as follows:

- Connect N.C. devices **in series** with the high (+) side of the loop. The 2K EOL resistor must be connected in series with the devices, following the last device.
- Connect N.O. devices **in parallel (across)** the loop. The 2K EOL resistor must be connected across the loop wires at the last device.

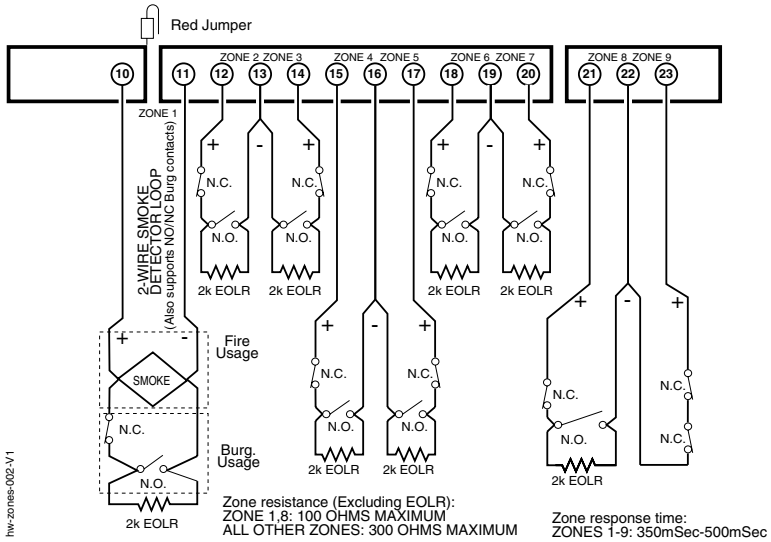


Figure 3-9: Wiring Connections for Zones 1-8

Using 2-Wire Smoke Detectors on Zone 1

Zone 1 can support up to 16 2-wire smoke detectors.

The alarm current on zone 1 supports only one smoke detector in the alarmed state.

Compatible 2-Wire Smoke Detectors

DETECTOR TYPE	DEVICE MODEL #
Photoelectric, direct-wire	System Sensor 2W-B
Photoelectric w/heat sensor, direct-wire	System Sensor 2WT-B
Ionization w/B401B base	System Sensor 1451
Photoelectric duct detect (DH400 base)	System Sensor 2451
Ionization duct detector (DH400 base)	System Sensor 1451DH
Ionization, direct-wire	System Sensor 1100
Photoelectric w/B110LP base	System Sensor 2151

UL These smoke detectors are UL Listed for use with the VISTA-128BPT/VISTA-250BPT and are the **only** 2-wire smoke detectors that may be used.

Wiring 2-Wire Smoke Detectors to Zone 1

2K EOL resistors must be used on fire zones and must be connected across the loop wires of each zone at the last detector.

To wire 2-wire smoke detectors to zone 1, perform the following steps:

Step	Action
1	Select up to 16 2-wire smoke detectors from the list of compatible detectors.
2	Connect 2-wire smoke detectors across zone 1 terminals (10 and 11) as shown in *Figure 3-10*. Observe proper polarity when connecting the detectors.
3	Connect the EOL resistor at the last detector in the loop across the zone 1 terminals. **The EOL resistor must be connected across the loop wires at the last detector.**

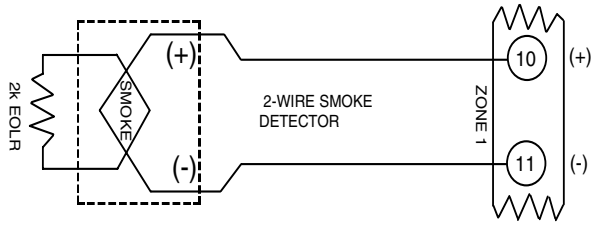


Figure 3-10: 2-Wire Smoke Detector on Zone 1

Using 4-Wire Smoke Detectors on Zone 1

You may use as many 4-wire smoke detectors as can be powered from the panel's Auxiliary Power output without exceeding the output's rating (750mA).

- NFPA limits the number of 4-wire smoke detectors to 18 per zone.
- Auxiliary power to 4-wire smoke detectors is not automatically reset after an alarm, and therefore must be momentarily interrupted using either the J7 smoke detector reset output trigger or a 4204 Relay Module.

Compatible 4-Wire Smoke Detectors

Use any UL Listed 4-wire smoke detector that is rated for 10-14VDC operation and that has alarm reset time not exceeding 6 seconds. Some compatible 4-wire smoke detectors are listed below.

Detector Type	Detector Model #
Photoelectric, direct wire	System Sensor 4W-B
Photoelectric w/heat sensor, direct wire	System Sensor 4WT-B

Wiring 4-Wire Smoke Detectors

UL Power to 4-wire smoke detectors must be supervised with an EOL device (use a System Sensor EOLR-1 EOL relay module connected as shown in *Figure 3-11*).

To wire 4-wire smoke detectors to zone 1, perform the following steps:

Step	Action
1	Select 4-wire smoke detectors (see list of compatible detectors shown previously).
2	Connect detectors (including heat detectors, if used) across terminals of the zone selected. All detectors must be wired in parallel. See *Figure 3-11*. **NOTE:** If you are using the J7 output trigger to reset the smoke detectors, refer to *Smoke Detector Reset* later in this section for the wiring instructions.
3	Connect the EOLR at the last detector in the loop across the zone's terminals. **You must connect the EOLR across the loop wires at the last detector**.

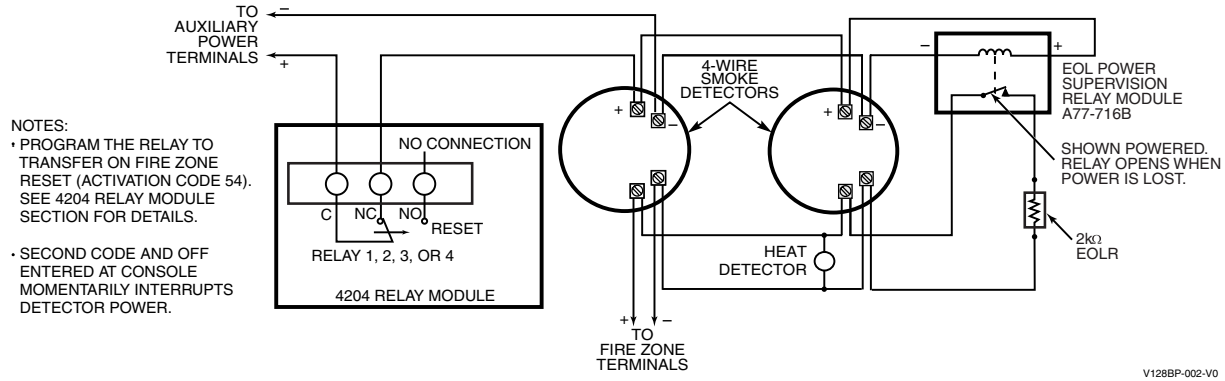


Figure 3-11: 4-Wire Smoke Detectors

Tamper Supervision for the Hardwired Zones

The system can be programmed to monitor for either an open condition or a short condition of a tamper switch on zones 1-8. End-of-line supervision is required for this option.

Wiring a Tamper Switch to Zones 1-8

The wiring of the tamper switch depends on whether the tamper switch and the sensor are normally open or normally closed.

- **If you are using a normally closed sensor,** the tamper switch must be normally open. Refer to *Figure 3-13* for the wiring configuration.
- **If you are using a normally open sensor,** the tamper switch must be normally closed. Refer to *Figure 3-14* for the wiring configuration.
- **For the normally closed sensor**, program the zone for trouble on short. **For the normally open sensor**, program the zone for trouble on open.

To wire a tamper switch on a hardwired zone, connect the EOL resistor at the last detector in the loop across the zone's terminals. **You must connect the EOL resistor at the last detector for proper operation of the tamper supervision.**

NOTE: These zones cannot be programmed for any 24 hour zone type and that tamper supervision is only in the disarmed state. When armed goes into alarm.

NOTE: For zones with a response type of 9 or 16 (Fire), the tamper selection must be "0" none.

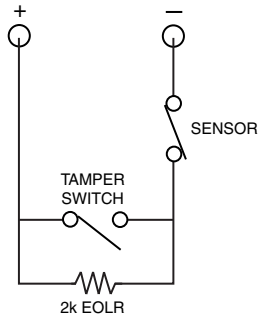


Figure 3-13: Wiring a Normally Closed Loop for Tamper Supervision

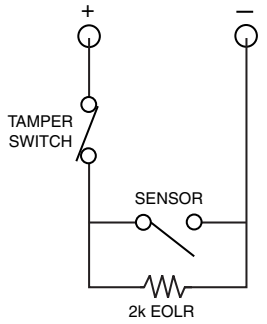


Figure 3-14: Wiring a Normally Open Loop for Tamper Supervision

Installing V-Plex Devices

The polling loop provides both power and data to the V-Plex devices, and is constantly monitoring the status of all zones enabled on the loop. The maximum current draw of all devices on the polling loop cannot total more than 128mA (unless the system uses a 4297 Polling Loop Extender Module).

Devices that can be programmed via either DIP switches or the built-in unique serial number **must** be set for the serial number mode operation.

All devices on the polling loop must be wired in parallel to the [+] and [-] polling loop terminals of the control panel (24 and 25). You can wire from device to device, or have multiple branches connected directly to the control panel in a star configuration.

Compatible Polling Loop Devices

Model Number	Type
4297	Extender Module
DT7500SN	V-Plex Dual Tech PIR
IS2500SN	V-Plex Dual Tech
4208SN	8 Zone V-Plex Interface
4208SNF	8 Zone V-Plex Class A Interface
269SN	V-Plex Holdup Switch
5192SD	Photoelectric Smoke Detector Devices
5192SDT	Photoelectric Smoke Detector w/Heat Detector
5193SD	Photoelectric Smoke Detector Device
5193SDT	Photoelectric Smoke Detector w/Heat Detector
4101SN	Serial Number Single-Output Relay Module
4208U	Universal 8-Zone Expander
4959SN	Aluminum Overhead Door Contact
4209U	Universal Group Zoning Module
4193SN	Serialized 2-Zone Expander
4293SN	Serialized 1-Zone Expander
4190SN	Serialized 2-Zone Expander
998MX	Serialized PIR
V-Plex VSI	V-plex Short Isolator

UL

- The 4208 must be mounted either inside the control panel's cabinet or in a separate enclosure that has a tamper-supervised cover.
- The 4190WH right loop must not be used, and the left loop must be EOLR-supervised.
- The 4278 right loop cannot be used.
- The 4297 must be powered from the control panel's Auxiliary Power Output or from a UL Listed supplementary power supply.

- For new polling loop installations, always use twisted pair wiring. In many cases, existing non-twisted pair wiring may be used, but it is more susceptible to interference from other sources, and may be problematic in installations with long wire runs or in high noise environments.
- Always locate polling loop wiring at least 6 inches (15cm) of AC power, telephone, or intercom wiring. The polling loop carries data between the control panel and the devices; interference on this loop can cause an interruption of communication. The polling loop can also cause outgoing interference on the intercom or phone lines. If this spacing cannot be achieved, shielded wire must be used. (Note that the maximum total wire length supported is cut in half when shielded wire is used.)

No more than 64mA may be drawn on any individual wire run.

IMPORTANT NOTE: If the installation needs to exceed or deviate from these parameters, refer to the application note on the Honeywell website for additional polling loop wiring configurations. To access the application note:

1. Go to the honeywell.com/security website
2. Click the Honeywell Security & Communications link.
3. Click the Commercial link.
4. Click the Documentation link.
5. Click the V-Plex Application Note.

To install polling loop devices, perform the following steps:

Step	Action
1	Select devices from the list of compatible devices shown previously.
2	Set the DIP switches in the device (if required). Refer to the device's instructions.
3	Mount each device in the desired location. Refer to the device's instructions.
4	Run wires from the control panel to each device on the polling loop (see *Figure 3-15*).
5	Wire each device to the polling loop, making sure of the correct polarity (refer to the device's instructions). **NOTE:** If you are using serial number devices, and intend to enroll each device through the keypad automatically, **wire no more than 25 of these devices to the control at a time.** Then power up and program them before connecting the next 25. Leave previously enrolled devices connected. If you intend to **manually enter the serial numbers** via the keypad or the Compass downloading software, all the devices may be connected before powering up to program.

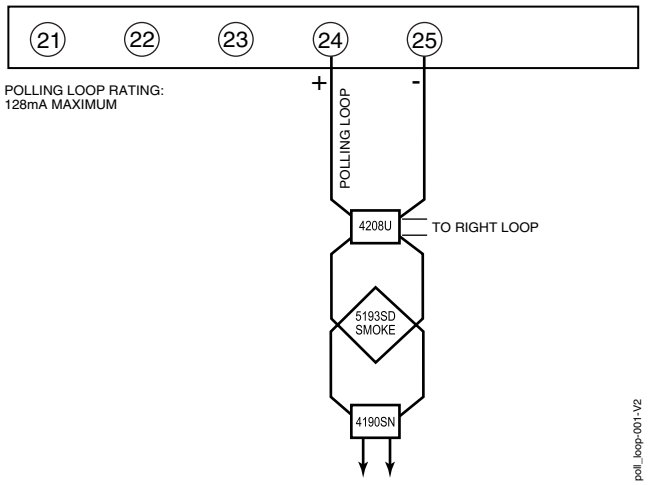


Figure 3-15: Polling Loop Connections to the VISTA-128BPT/VISTA-250BPT

Polling Loop Supervision

A short on the polling loop is indicated by a trouble on zone 997 and reports as a trouble condition only. If annunciation is desired, program the zone as type 05.

If a device on the polling loop fails (the panel cannot "see" that device), the system displays a trouble condition for all zones on that device. If the panel is armed when a device fails, and the zone is a burglary zone, the will go into alarm

A trouble on zone 997 prevents a partition from being armed, unless all polling loop zones on that partition are bypassed.

Using the 4297 Polling Loop Extender

The 4297 Polling Loop Extender may be used to provide additional polling loop current, to extend the polling loop wire run length, and/or to provide individual electrically isolated polling loops. Refer to *Figures 3-16 and 3-17*, to follow.

DO NOT use the 4197 Polling Loop Extender module with the VISTA-128BPT/VISTA-250BPT.

Be sure to include the total current drawn on the polling loop when figuring the total auxiliary load on the panel's power supply.

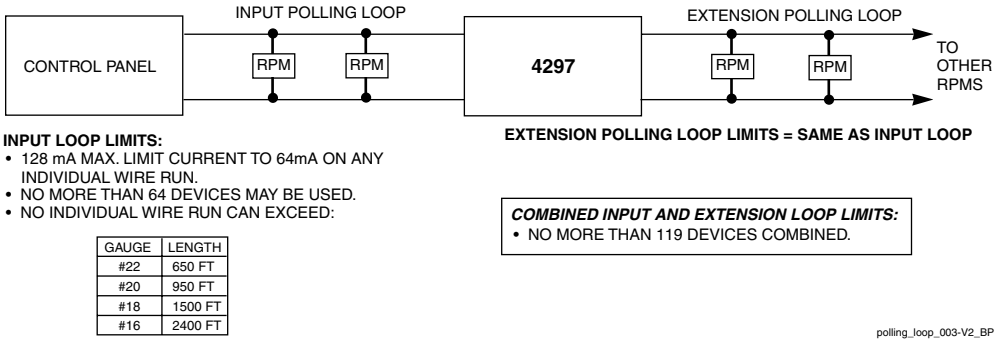


Figure 3-16: Polling Loop Connections Using One 4297 Extender Module

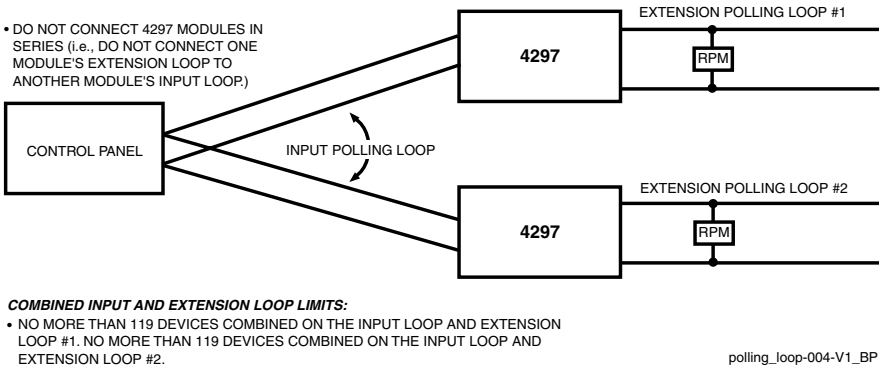


Figure 3-17: Polling Loop Connections Using Multiple Extender Modules

NOTE: The input loop limits stated in *Figure 3-16* apply to *Figure 3-17* as well.

Wireless Zone Expansion

UL The 5881ENHC RF Receiver, 5869 Holdup Switch Transmitter and 5817CB Wireless Commercial Household Transmitter are listed for UL Commercial Burglary applications. All other RF receivers and transmitters are not listed for UL Commercial Burglary applications.

ULC Wireless devices are not ULC Listed and cannot be used for ULC Installations.

The following table lists the receivers that may be used and the number of zones they support.

5800 Series Receivers

Receiver	Zones
5881ENHC	up to 250

RF System Operation and Supervision

The 5800 RF system operation has the following characteristics:

- The receiver responds to a frequency of 345MHz.
- The receiver has a nominal range of 200 feet.
- Supervised transmitters send a supervisory signal every 70-90 minutes.
- Zones 988 and 990 are used to supervise the RF reception of receivers 2 and 1, respectively. The reception is supervised for two conditions:
  1. The receiver goes "deaf" (doesn't hear from *any* transmitter) within a programmed interval of time (defined by program field 1*30).
  2. Proper RF reception is impeded (i.e., jamming or other RF interference). The control checks for this condition every 45 seconds.

UL A response type (05 Day/Night) must be programmed for zones 990 (1st receiver) and 988 (2nd receiver) for UL installations.

- The 5881ENHC receiver contains front and back tampers that permit its use in commercial burglary installations.
- You may only mount the 5881ENHC its own plastic housing. Otherwise, the receiver constantly reports a tamper condition.
- The control checks the receiver connections about every 45 seconds. The receiver supervisory zone is 8 + 2-digit receiver device address (for example, Device address 05 = supervisory zone 805).

  NOTE: This zone must be programmed with a response type (e.g., type 05 Day/Night Trouble) before it supervise the connection to the receiver.
- Use two identical receivers to provide either a greater area of coverage or redundant protection. They must be set for different addresses.

  NOTE: No more than two receivers can be installed.
- Any zone from 1 to 250 can be used as a 5800 Series wireless zone, with the exception of zone 64 (reserved for a wireless keypad).

RF System Installation Advisories

UL The 5827 and 5804BD are not UL Listed and are not intended for use in UL Listed applications.

- Place the receiver in a high, centrally located area. Do not place it on or near metal objects. This will decrease the range and/or block transmissions.
- Install the RF receiver at least 10 feet from the control panel or any keypads, to avoid interference from the microprocessors in these units.
- If dual receivers are used:
  a. They must be at least 10 feet from each other, as well as from the control panel and remote keypads.
  b. Each receiver must be set to a different device address. The receiver set to the lower address is considered the 1st RF receiver for supervisory purposes.
  c. The House IDs must be the same.
  d. Using two receivers *does not* increase the number of transmitters the system can support (249 zones using the 5881ENHC, plus a wireless keypad).

Installation and Setup of 5881ENHC RF Receivers

Take note of the address you select for the RF receiver, as this address must be enabled in the system's *Device Programming* in the *#93 Menu Mode*.

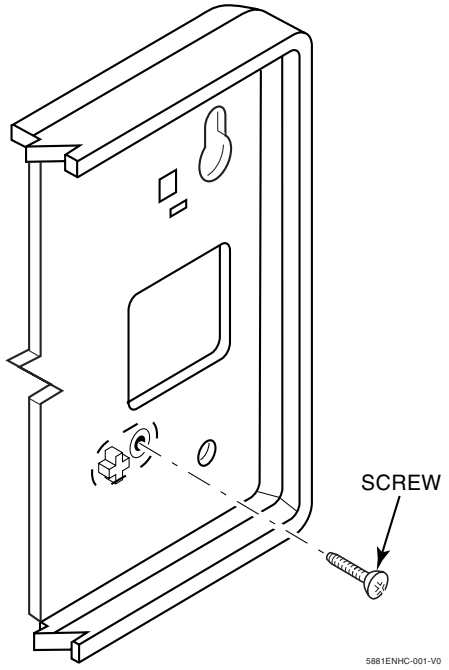


Figure 3-18: Installing the 5881ENHC with Tamper Protection

To install the 5881ENHC RF receiver, perform the following steps:

Step	Action
1	Mount the receiver, following the advisories stated previously.
2	Set the DIP switches in the receiver for the address **(01-07)**. See *Figure 3-19*. **Make sure the address setting is not being used by another device (keypad, relay module, etc.).**
3	If installing a 5881ENHC, install a flat-head screw (supplied) in the case tamper tab as shown in *Figure 3-18*. When the receiver is pried from the wall, the tamper tab will break off and remain on the wall. This will activate a tamper switch in the receiver and cause generation of a tamper signal. Note that this signal will also be generated when the receiver's front cover is removed.
4	Connect the receiver's wire harness to the keypad terminals (6, 7, 8, and 9). Plug the connector at the other end of the harness into the receiver.

5	Refer to the Installation Instructions provided with the receiver for installations regarding antenna mounting, etc.

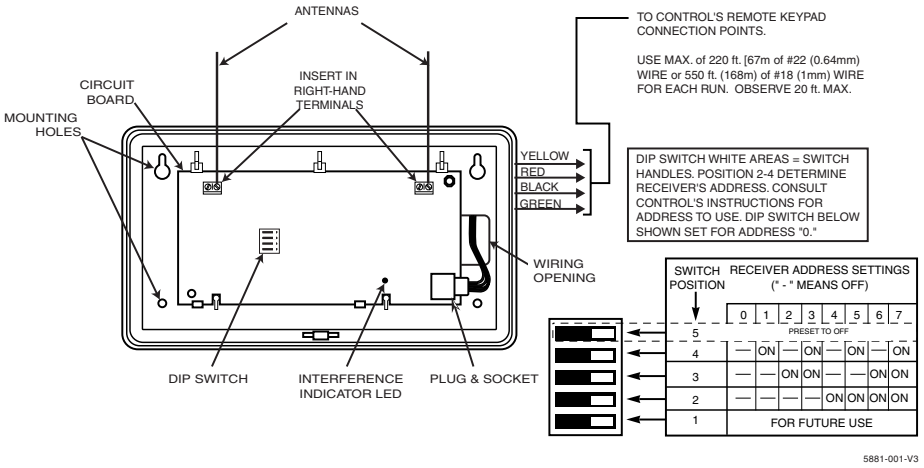


Figure 3-19: 5881ENHC RF Receiver (cover removed)

Installing the 5800TM Module

Installation of this module is necessary only if you are using a 5804BD Bi-directional device.

The address for the 5800TM must be enabled in the control's *Device Programming* in the *#93 Menu Mode* as a keypad and then assigned to a partition.

To install the 5800TM, perform the following steps:

Step	Action
1	Mount the unit using its accompanying mounting bracket near the RF receiver. **The 5800TM must not be installed within the control cabinet. It must be between one and two feet from the receiver's antennas.**
2	Set the module for the appropriate address. For Address Setting 28 cut the red jumper; for Address 29 cut the white jumper; for Address 30 cut both jumpers. **Make sure the address setting is not being used by another device (keypad, relay module, etc.).**
3	Connect the module's wire harness to the keypad terminals (6, 7, 8, and 9). Plug the connector at the other end of the harness into the module.

House ID Sniffer Mode

This mode applies only if you are using a wireless keypad (e.g., 5827) or bi-directional devices (e.g., 5804BD). Use the House ID Sniffer mode to make sure you do not choose a House ID that is in use in a nearby system. The House ID must be programmed for the receiver in *Device Programming* in the *#93 Menu Mode*.

To enter House ID Sniffer mode, enter your **Installer Code + [#] + [2].**

The receiver now "sniffs" for any House IDs in the area and displays them. Keep the receiver in this mode for 2 hours. Use a House ID that is not displayed. Exit the Sniffer mode by entering your **Installer Code + OFF**.

As Sniffer mode effectively disables RF point reception, Sniffer mode **cannot** be entered while any partition is armed.

5800 Series Transmitter Setup

5800 Series transmitters have the following characteristics:

- Transmitters have built-in serial numbers that must be enrolled in the system using the *#93 Menu Mode Programming*, or input to the control via the downloader.
- Transmitters do not have DIP switches (except 5827, described separately).

- Some transmitters, such as the 5816 and 5817, can support more than one "zone" (referred to as loops or inputs). Each loop must be assigned a different zone number.
- For button-type transmitters (wireless keys), such as the 5804 and 5804BD, you must assign a unique zone number to each individual button used on the transmitter.

Transmitter Input Types

All transmitters have one or more unique factory-assigned input (loop) codes. Transmitters can be programmed as one of the following types:

Type	Description
RM (RF Motion)	Sends periodic check-in signals, as well as fault and low-battery signals. The control panel automatically restores the zone to "ready" after a few seconds. This type is designed for facilities with multiple motion detectors that may fault and restore simultaneously. The transmitter must remain within the receiver's range. **NOTE:** If using RF Motion with a door/window type transmitter, only loop 1 may be used.
RF (Supervised RF)	Sends periodic check-in signals, as well as fault, restore, and low-battery signals. The transmitter must remain within the receiver's range.
UR (Unsupervised RF)	Sends all the signals that the RF type does, but the control does not supervise the check-in signals. The transmitter may therefore be carried off-premises.
BR (Unsupervised Button RF)	These send only fault signals. They do not send low-battery signals until they are activated. The transmitter may be carried off-premises.

Transmitter Supervision

Supervised RF transmitters send a check-in signal to the receiver at 70–90 minute intervals. If at least one check-in is not received from each supervised transmitter within a programmed period (field 1∗31), the "missing" transmitter number(s) and "CHECK" or "TRBL" are displayed. Unsupervised RF transmitters (5802MN, 5804) may be carried off the premises.

Some transmitters have built-in tamper protection, and annunciate a "CHECK" or "TRBL" condition if covers are removed.

If a loss of supervision occurs on a transmitter programmed for Fire, it reports in Contact ID as a Fire Trouble (373), not Loss of Supervision (381), to the central station.

Transmitter Battery Life

Batteries in the wireless transmitters may last from 4 to 7 years, depending on the environment, usage, and the specific wireless device being used. Factors such as humidity, high or low temperatures, as well as large swings in temperature may all reduce the actual battery life in a given installation.

The wireless system can identify a true low battery situation, thus allowing the dealer or user of the system time to arrange a change of battery and maintain protection for that point within the system.

Button-type transmitters (e.g., 5802, 5804 and 5805-6) should be periodically tested, as these transmitters do not send supervisory check-in signals.

To test the transmitters using the Transmitter ID Sniffer mode and the Go/NoGo Test Mode, see *SECTION 10: Testing the System* for the procedures.

Compatible 5800 Series Transmitters

Model	Product	Input Type
5800CO	Carbon Monoxide Detector with Built-in Wireless Transmitter	RF
5800RP	RF Repeater Module	RF
5802 5802CP	Pendant (Personal Emergency Transmitter) Belt Clip (Personal Emergency Transmitter)	BR Only
5802MN	Miniature (Personal Emergency Transmitter)	UR or RF
5802MN2	Miniature (Personal Emergency Transmitter)	UR or RF
5804	Wireless Key Transmitter	BR Only
5804BD	Wireless Key Bi-directional Transmitter	BR Only
5804BDV	Wireless Key Bi-directional Transmitter with Voice	BR Only

5808W3	Wireless Photoelectric Smoke Detector	RF
5816	Door/Window Transmitter	RF
5817	Multi-Point Universal Transmitter	RF
5817CB	Wireless Commercial Household Transmitter	RF
5818	Recessed Transmitter	RF
5827	Wireless Keypad	House ID
5827BD	Wireless Bi-directional Keypad	House ID
5800PIR-COM	PIR Detector	RF
5800PIR	PIR Detector with Pet Immunity	RF

Installing Output Devices

The VISTA-128BPT/VISTA-250BPT support up to 96 outputs. Each device must be programmed as to how to act (ACTION), when to activate (START), and when to deactivate (STOP). The 4204, 4101SN and/or X-10 devices may be used as output devices.

Installing a 4204 Relay Module

ULC Relay modules have not been evaluated for ULC installations.

Each 4204 module provides 4 relays with Form C (normally open and normally closed) contacts.

The relay module will not operate until the device address you have set the DIP switches for is enabled in the control's *Device Programming* in the *#93 Menu Mode*.

To install the relay modules, see *Figure 3-20 and* perform the following steps:

Step	Action
1	Set the 4204 DIP switches for a device address **01-15**. Do not use an address being used by another device (keypads, RF receivers, etc.).
2	Mount the 4204 Module per the instructions provided with them.
3	Connect the module's wire harness to the control (6, 7, 8, and 9). Plug the connector (other end of harness) to the module. If you are mounting remotely, homerun each module to the control. The table below shows the maximum wire run lengths.

Wire Gauge	Maximum Length
#22	125 feet
#20	200 feet
#18	300 feet
#16	500 feet

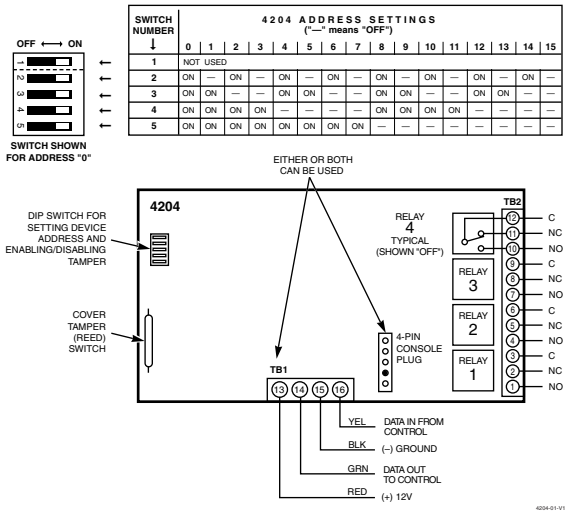


Figure 3-20: 4204 Relay Module

Installing 4101SN Relay Modules

The 4101SN V-Plex Single Output Relay Module is a serial number polling loop output device. The 4101SN features the following:

- Form C relay contacts rated at 2A, 28VAC/VDC with contact supervision.

The position of the relay is supervised, but not the actual external contact wiring.

- One class B/style B EOLR-supervised auxiliary input zone.
- Operating power and communication with control panels via the V-Plex polling loop.
- Electronics mounted in a small plastic case with tamper-protected cover.

Connect the device to the polling loop, terminals 24 (+) and 25 (-). Be sure to observe polarity

Installing X10 Devices

X-10 devices are either plugged into standard AC outlets or wired into the AC electrical system by a licensed electrician, depending on the type of device used.

UL X10 Devices are not permitted in UL installations.

Note each device's House and Unit Code setup, as these codes will be used to program the devices in *Output Programming* in *#93 Menu Mode* described in the *Programming Guide*.

X-10 devices require the use of a 1361X10 transformer in place of the regular 1361 transformer.

X-10 devices respond to "on" and "off" commands sent from the panel through the 1361X10 transformer.

To connect the 1361X10 transformer, see *Connecting the Transformer,* later in this section.

Installing a Remote Keyswitch

A UL-Listed remote keyswitch, such as the ADEMCO 4146, can be used for remote arming/disarming of the burglary portion of the system and for silencing alarms. The keyswitch can operate in only one particular partition.

ULC Remote Arming is not a ULC Listed feature.

The keyswitch is wired across zone 7. This zone is no longer available as a protection zone. Be sure to program Zone 7 with a response type (e.g., type 10).

Operation

- A momentary short across zone 7 arms the partition in the AWAY mode, and a short held for more than 10 seconds arms the partition in STAY mode 1. A subsequent short disarms the partition.
- The keyswitch LEDs indicate the partition's status (see table below).
- A momentary short across Zone 7 silences alarm bell and keypad sounds, and disarms the system if it was armed. A subsequent short across Zone 7 clears the alarm memory indication and resets 2-wire smoke detectors (if used).

LED Indications

Green	Red	Indication
On	Off	Disarmed & Ready
Off	Off	Disarmed & Not Ready
Off	On Steady	Armed Away
Off	Slow Flash	Armed Stay
Off	Rapid Flash	Alarm Memory

The keyswitch reports as user 0, if Open/Close reporting is enabled in field ✳40.

Keyswitch Tamper Operation

The tamper switch need not be used for fire or UL Household Burglary installations. For UL Commercial Burglary installations, the tamper switch must be wired to a zone (zone 7 in *Figure 3-21*).

Program that zone for Day Trouble/Night Alarm (response type 5). When the keyswitch is removed from the wall, the tamper switch opens, causing an alarm or trouble on the zone. This also causes the control to disable keyswitch operation until the tamper is restored and the associated partition is disarmed.

Wiring for the Remote Keyswitch

To install the ADEMCO 4146 keyswitch, perform the following steps:

Step	Action
1	Connect the ADEMCO 4146 to the panel as shown in *Figure 3-21*.
2	If you are using the tamper, make sure it is connected to a zone.

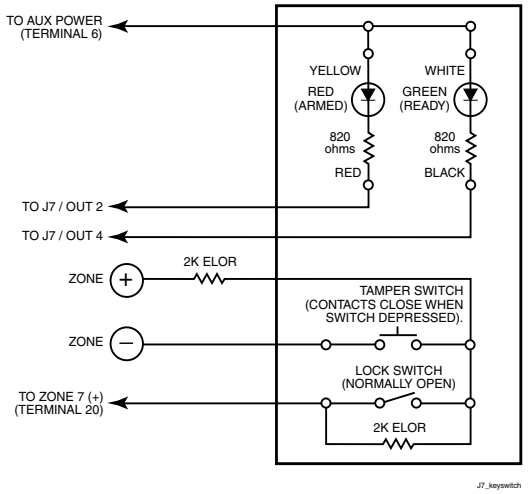


Figure 3-21: Remote Keyswitch Wiring

Smoke Detector Reset

Output 1 may be used to reset 4-wire smoke detectors. Use this output to trigger a low current relay, and wire the power for the smoke detectors through the relay's contacts.

NOTE: The output is normally high (12VDC) and goes low when the User Code + Off is entered at the keypad.

To install a relay for smoke detector reset, perform the following steps:

Step	Action
1	Connect power terminals of the relay to the panel's auxiliary power (terminals 6 & 7).
2	Connect trigger input of the relay to Output 1 on J7.
3	Connect the "pole" (common) of the relay to terminal 6 of the control.
4	Connect the positive side of the smoke detectors to the normally closed contact of the relay.
5	Connect the negative side of the smoke detectors to terminal 7 of the control.

Remote Keypad Sounder

This feature is available in the VISTA-128BPT and VISTA-128BPTSIA only. An optional Amseco PAL 328N Piezo Sounder can be used to duplicate the sounds produced by the keypad's built-in sounder. The panel will remote all sounds (e.g., alarm, trouble, chime, entry/exit, etc.) produced by the keypad's built-in sounder except for the short beeps associated with keypad key depression. One application of this feature might be to produce chime sounds at a distant location from the panel's keypads.

Remote Keypad Sounder Setup

To setup for a remote keypad sounder, connect the piezo sounder to the panel's positive auxiliary power output and to Output 1 on the J7 connector as shown in *Figure 3-22*.

To duplicate the keypad sounds for a particular partition, program that partition number in field ✳15.

Program field 1✳46 Auxiliary Output Enable with a [**2**].

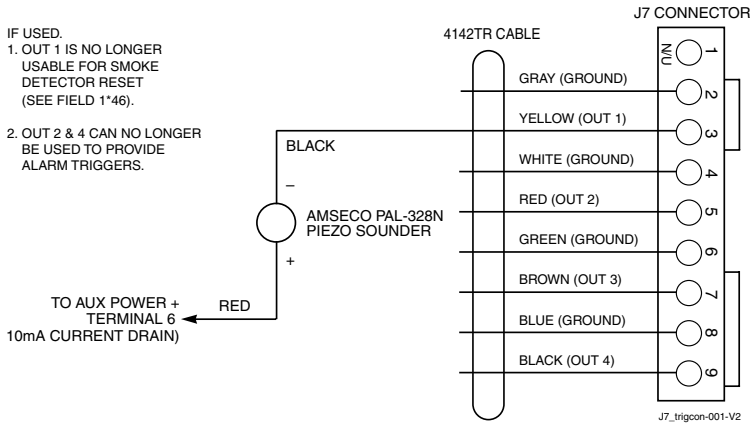


Figure 3-22: Remote Keypad Sounder Wiring

Communicators Connected to the ECP

The control can support an ECP Communicator (such as the 7845GSM, 7845i-GSM, and 7845i-ent) that connects to control panel's keypad terminals. All messages programmed for transmission via the phone lines may also be sent via the Communicator. These messages are transmitted in Contact ID format regardless of the format programmed for the control in fields 45 and 47.

We recommend that, if possible, you use Contact ID for the main dialer. If Contact ID is not used, certain types of reports are not sent.

ULC For ULC installations, Contact ID is the only permitted format.

Operation

The VISTA-128BPT/VISTA-250BPT features **Dynamic Signaling Delay** and **Dynamic Signaling Priority** message reporting when a Communicator is used. These options are accessed through data fields ∗56 and ∗57, respectively. The Dynamic Signaling feature is designed to reduce the number of redundant reports sent to the central station.

The feature is described as follows:

Dynamic Signaling Delay (Field ∗56)

Select the time the panel should wait for acknowledgment from the first reporting destination before it attempts to send a report to the second destination. Delays can be selected from 0 to 225 seconds, in 15-second increments.

Dynamic Signaling Priority (Field ∗57)

Select the initial reporting destination for reports, Primary Dialer **(0)** or Communicator **(1)**.

The chart below provides an explanation of how the Dynamic Signaling feature functions.

If Priority (∗57) is…	And message is…	Then…
Primary Phone No. ("0")	Acknowledged before delay expires	Report is removed from queue and no message is sent to Communicator.
	Not acknowledged before delay expires	Report is sent to both the Primary Phone No. and Communicator.
Long Range Radio ("1")	Acknowledged before delay expires	Report is removed from queue and no message is sent to Primary Phone No.
	Not acknowledged before delay expires	Report is sent to both the Primary Phone No. and Communicator.

Additional Communicator reporting options are defined by selecting the events for each subscriber ID in fields 58 and 59. The reporting events are Alarms, Troubles, Bypasses, Openings/Closing, System Events, and Test. Also, within an enabled category, the specific event must be enabled for dialer reporting. If, for instance, zone 10 is enabled to report, but zone 11 is not, zone 10 will report via the Communicator, but Zone 11 will not.

Reports are transmitted from the VISTA-128BPT/VISTA-250BPT to the Communicator on a "first in/first out" basis. If events occur at the same time, they are transmitted in order of priority. The priority from most to least important is : Fire Alarms, Panic Alarms, Burglary Alarms, Fire Troubles, Non-Fire Troubles, Bypasses, Openings/Closings, Test messages, and all other types of reports.

There are two subscriber IDs programmed into the Communicator: primary and secondary. These correspond to the two subscriber ID's programmed into the control for each partition. If a subscriber ID for a partition is not programmed (disabling reports to that central station), the events enabled for the corresponding subscriber ID in the Communicator will not be transmitted.

If the event is to be reported to both phone numbers (dual reporting), then reporting through the Communicator will be done in an alternating sequence. The first event in the queue is transmitted to both the primary and the secondary Communicator central stations before transmitting the second event.

If split reporting is selected for the VISTA-128BPT/VISTA-250BPT, then the Communicator will send the appropriate reports to the primary and secondary central stations.

Installing the ECP Communicator

To install the ECP Communicator, perform the following steps:

Step	Action
1	Mount the Communicator according to the instructions that accompany the Communicator.
2	Connect the data in/out terminals and voltage input terminals of the Communicator to the control's keypad connection points, terminals 6, 7, 8, and 9. See *Figure 3-23*.

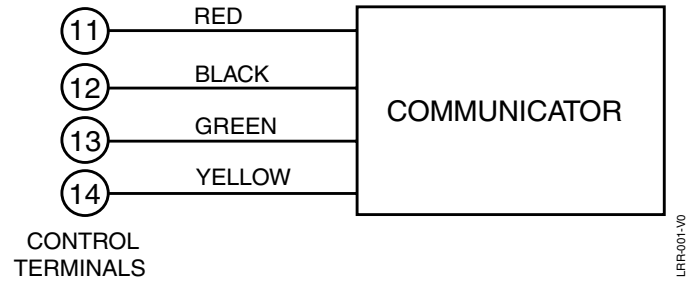


Figure 3-23: Wiring the Communicator to Keypad Terminals

Supervision

The data lines between the control and the Communicator, as well as certain functions in the Communicator, can be supervised.

If communication is lost or a trouble condition occurs, both the Communicator and the control's dialer can be programmed to send a Trouble message to the central station.

NOTE: For complete information, see the Installation Instructions that accompany the Communicator.

Trouble Messages

The following messages are displayed on the 6160 when a problem exists on the Communicator:

1. "LRR Battery": The battery connected to the Communicator is low.
2. "PLL out of Lock": The Communicator has an internal fault and cannot transmit any messages.
3. "Early Power Detect": RF power is detected without a valid transmission.
4. "Power Unattained": Full RF power was never attained.
5. "Frwd. Power Loss": RF power was not sustained throughout the transmission.
6. "Antenna Fault": A problem with the antenna has been detected.
7. "LRR CRC is bad": The Communicator's EEPROM is corrupt (the internal CRC is bad).

NOTES:

Items 2 and 3 require factory service.

Items 4 and 5 could be the result of a bad or low battery.

If the item 6 message appears, check the antenna, connection and cable; if they are secure, factory service is required.

All these messages are displayed in conjunction with the "CHECK 8xx" message, which indicates a trouble on the address to which the Communicator unit is programmed in the control.

All of these events except Antenna Fault are sent to the event log and reported to the central station using Contact ID Event Code 333 (expansion device trouble). Antenna Fault uses Event Code 357. If the tamper is tripped on the Communicator, it uses Event Code 341 (expansion device tamper).

Access Control Using VistaKey

The VistaKey is a single-door access control module that, when connected to the alarm system, provides access control to the protected premises. The VISTA-128BPT supports up to 8 modules, the VISTA-250BPT supports up to 15 VistaKey modules (15 access points).

UL The VistaKey module contains three zones. These zones should ONLY be used for access control functions in UL installations. THESE INPUT ZONES ARE NOT TO BE USED FOR FIRE AND BURGLARY APPLICATIONS IN UL INSTALLATIONS.

VistaKey Features

- Each VistaKey communicates with the VISTA-128BPT/VISTA-250BPT via the V-Plex polling loop.
- In the event local power to the VistaKey is lost, the VistaKey module provides backup monitoring of the access point door via a built-in V-Plex device that is powered solely from the polling loop. It is programmed as a new type of V-Plex device as part of the control's V-Plex Device Programming. A serial number label is affixed to the VistaKey module for manual entry of its serial number.
- The VistaKey supports up to 500 cardholders.
- The addition and removal of VistaKey modules from the system is easily accomplished via the VISTA-128BPT/VISTA-250BPT keypad.
- All configurable options for each VistaKey are accomplished via software, firmware, and nonvolatile memory, eliminating the need for PC board jumpers. The access point zone number (1-15) is set via a user-friendly, 16-position rotary switch.
- Each VistaKey provides one open-collector output trigger (sink 12mA @ 12VDC).

Mounting and Wiring the VistaKey

For detailed instructions on how to install and program the VistaKey, refer the *Installation and Setup Guide* that accompanies the VistaKey-SK.

To mount and wire the VistaKey module, perform the following steps:

Step	Action
1	Mount the VistaKey, door strike or mag lock, and card reader.
2	Mount the door status monitor (DSM) and/or request-to-exit (RTE) devices.
3	Using *Figure 3-24* as a reference, connect the card reader interface cable to TB3, *making the +5V or +12V connection last*.
4	Connect the leads to TB1 in the following order: a. All ground leads to terminals 2, 5, and 9. b. The DSM, (optional) RTE, and General Purpose leads to terminals 6, 7, and 8, respectively. c. Door strike (or mag lock) lead to terminal 10. d. Local +12V or +24V supply lead to terminal 1. e. Local +12V or +24V supply lead to the N/C relay terminal 11 (if a mag lock is being used), **OR** to the N/O relay terminal 10 (if a door strike is being used).
5	Connect the (–) polling loop and (+) polling loop leads (from the VISTA-128BPT/VISTA-250BPT) to terminals 4 and 3, respectively.
6	Set the Address Select switch to the desired access door number (1-15).
7	Repeat steps 1 through 6 for each VistaKey being installed.

Connecting the Card Reader

Lead from Reader	Lead Color	To VistaKey TB3 Terminal #
Green LED	Orange	1
Ground*	Black	2
DATA 1 (Clock)	White	3
DATA 0 (Data)	Green	4
+5VDC†	Red†	6
+12VDC†	Red†	7
* TB-3 Terminal 5 is also a ground and may be used instead of terminal 2. Terminals 2 and 5 are a common ground. † Connect to +5VDC OR +12VDC per reader manufacturer's specification.		

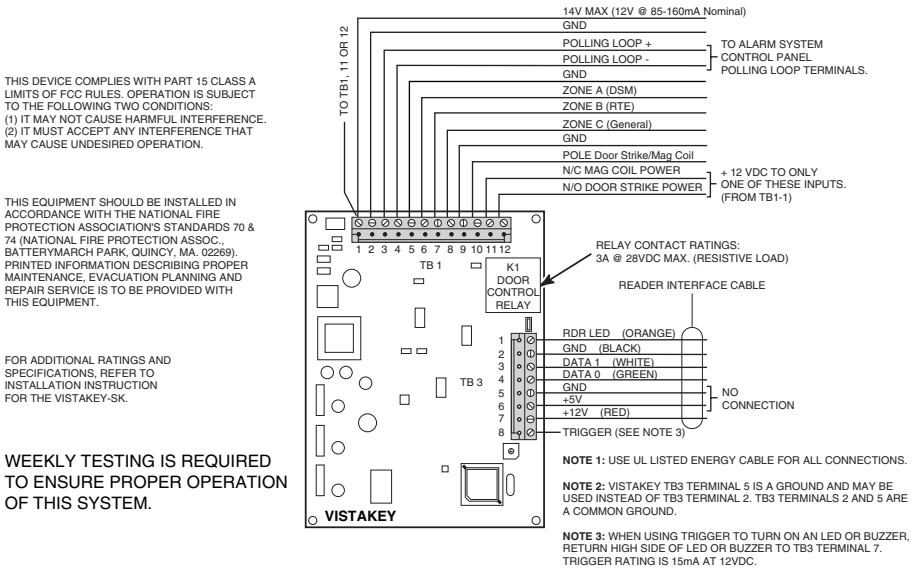


Figure 3-24: Wiring the VistaKey

Installing the 4286 VIP Module

The 4286 VIP Module is an add-on accessory that permits the user to access the security system (and relays) via a TouchTone telephone. This may be done either from the premises or by calling the premises from a remote location. Only one VIP Module can be used in a security system. This module must be enabled as Device Address 4 in the *Device Programming* in *#93 Menu Mode*, and must be assigned to a partition.

UL The 4286 VIP Module is not permitted in UL installations.

Detailed operating instructions for phone access to the security system are provided with the VIP Module.

The 4286 VIP Module features:

- Allows the user to receive synthesized voice messages over the phone regarding the status of the security system.
- Allows the user to arm and disarm the security system and perform most other commands using the telephone keypad.
- Allows the user to control relays using the telephone keypad.
- Provides voice annunciation over the phone to confirm any command that is entered.
- Announces many of the same words that would normally be displayed on an alpha keypad under the same system conditions. Refer to the words in bold on the Alpha Vocabulary list found in the *#93 Menu Mode* in the *Programming Guide*.
- Can be supervised for connection to control panel (annunciated and reported as Zone 804).

The 4286 is wired between the control panel and the premises' handset(s) (see *Figure 3-25*). It listens for TouchTones on the phone line and reports them to the control panel. During on-premises phone access, it powers the premises phones. During off-premises phone access, it seizes the line from the premises phones and any answering machines.

- The VIP module will not operate until the device address (04) is enabled in the control's *Device Programming* in *#93 Menu Mode*.
- Do not mount the VIP Module on the cabinet door or attempt to attach it to the PC board.

To install the VIP module, perform the following steps:

Step	Action
1	Mount the module in the control cabinet if space is available or, if this is not possible, on the side of the cabinet or adjacent to it. **If you mount the VIP Module inside the control cabinet,** attach it to the cabinet's interior surface with 2-faced adhesive tape. You may leave the module's cover off if it is mounted within the cabinet. **If you mount the module outside the cabinet,** use the screw holes at the rear to mount horizontally or vertically (2-faced adhesive tape may be used, if preferred).
2	Affix the 4286 connections label (supplied separately) to the inside of the VIP Module's cover, if the cover is used. Otherwise, affix the label to the inside of the *control cabinet's* door.
3	Make 12V (+) and (–) and data-in and data-out connections from the VIP Module to the control, using the connector cable supplied with the VIP Module. These are the same connections as for remote keypads.
4	Connect the module to the phone line as shown below. See *Figure 3-25*.

	4286 Terminal	Connects to direct connect cord:	
	1. Phone In (Tip)	green wire	
	2. Phone In (Ring)	red wire	
	3. Phone Out (Tip)	brown wire	
	4. Phone Out (Ring)	gray wire	
	5. No Connection		
	6. Audio Out 1*	Speaker	
	7. Audio Out 1*	Speaker	

***Supported by the 4286 only**

Use an RJ31X Jack with the phone cable supplied with the control to make connections to the VIP module. Make connections exactly as shown in *Figure 3-25*. **This is essential, even if the system is not connected to a central station. The 4286 will not function if this is not done.**

- If touch-tones are not present following phone access to the security system *via an on-premises phone*, try reversing the pair of wires connected to terminals 3 and 4 on the 4286.
- If the phone plug is disconnected from the control, the premise's phones will not operate.

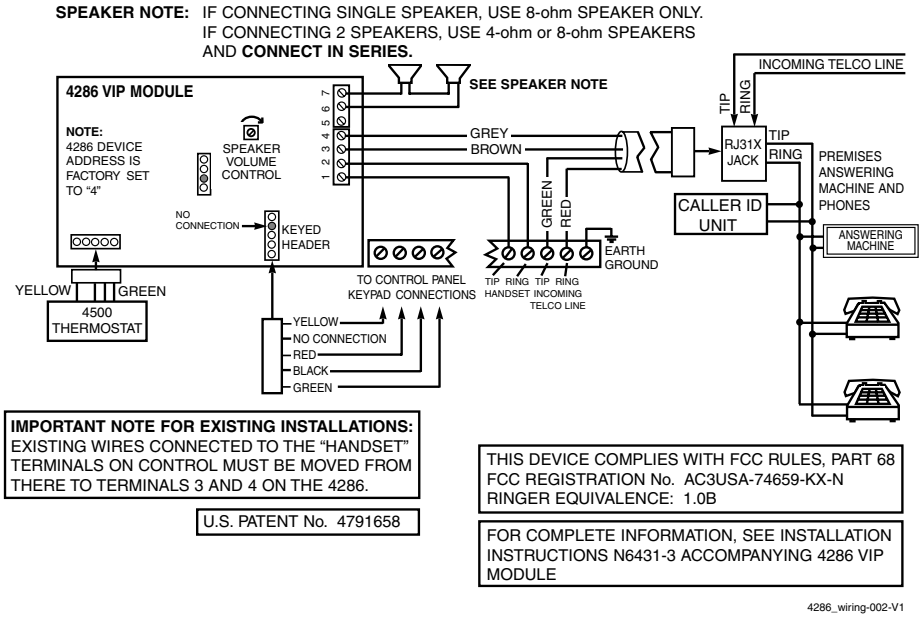


Figure 3-25: VIP Module Connections

Installing the Audio Alarm Verification Module

UL Audio Alarm Verification (AAV) is not permitted in UL installations.

- Contact ID code for "Listen-in to Follow" is 606. Contact ID is the only reporting format that will send a "Listen-in to Follow." It is the only format capable of uniquely reporting all 250 zones, as well as openings and closings for all 250 users. This requires central stations to be equipped with the MX8000 receiver to fully support all new report codes. If you need to update your MX8000 receiver, contact your distributor.
- If you are also using a 4286 VIP Module, be sure to follow *Figure 3-26* when making connections.

The UVS consists of a UVCM and at least one UVST. The UVCM board has a DC power jack and a 34-position terminal block for making connections to a DC power source, UVSTs, telephone lines, music source, or to the 4286 VIP Module; and to a control panel's voice trigger and bell outputs (if required). Refer *Figure 3-34* for wiring connections. For a detailed explanation of the wiring connections and the functions of the DC power jack and terminal block positions, refer to the installation instructions that accompany the UVS.

If the phone plug is disconnected from the control, the premise's phones will not operate.

NOTES:

- When the AAV indicates that the audio alarm verification session is completed, all keypad sounds are restored. Sirens are restored if the alarm timeout period has not expired.
- As part of its fail-safe software, the control limits all audio alarm verification sessions to 15 minutes. This is because once the session begins, the AAV Module controls the duration.
- If a new **Fire alarm** should occur during a session, the control breaks the phone connection and sends the new Fire Alarm report, then re-triggers the AAV Mode. All other dialer messages triggered during ongoing conversation are held until either the AAV Module signals that it is inactive, or the 15-minute timeout occurs.

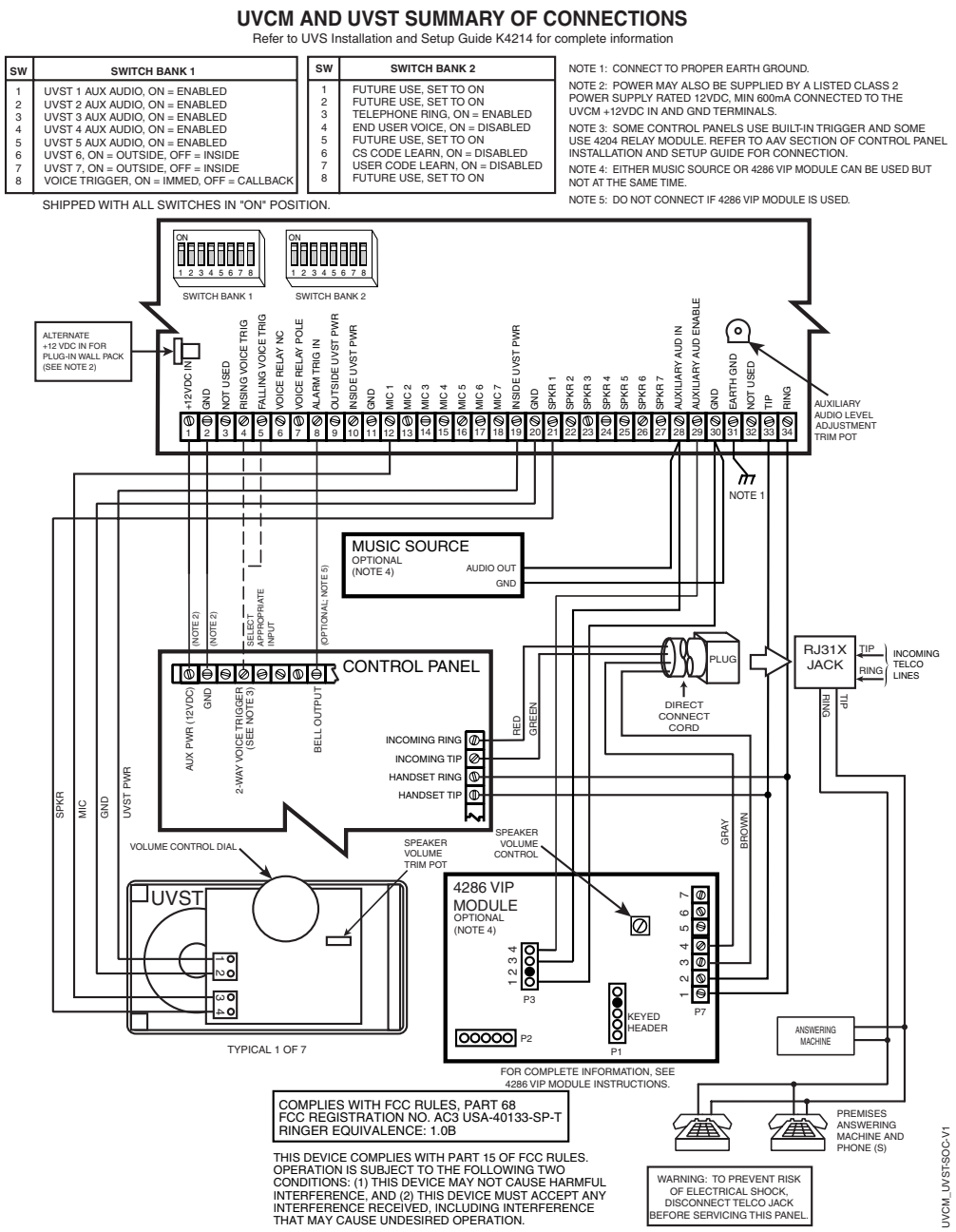


Figure 3-26: UVS Connections to the Control Panel

Connecting the Transformer

This product uses the 1361 transformer (1361CN in Canada). If you are using X-10 devices, the 1361X10 transformer interface must be used ***instead*** of the regular 1361 transformer. The 1361X10 supplies the control panel with AC, and also sends control pulses through the premises' electrical system to control the X-10 devices.

NOTE: For Canadian controls,upon a total power failure, the control unit will ignore and not transmit alarm supervisory information for a stabilization period of 120 seconds following restoration of power. Within 60 seconds at the end of the stabilization period, the control unit shall initiate the transmission of a power restoration signal code. If this report code is enabled (see report code programming in the Programming Guide), this is the report that will be sent.

UL Use 1361CN Transformer in Canadian installations.

Power Limiting Outputs

All outputs are power-limited as per UL985/UL1023. The following table shows the maximum current that may be drawn from each output.

Output	Maximum Current Draw
Auxiliary Power	750mA
Polling Loop	128mA
Alarm Output	1.7A

For Household Fire or Combination Household Fire/Burglary Installation: The total current drawn from the auxiliary power, the polling loop, and the alarm output combined must not exceed 750mA to comply with the battery independence requirements in UL985.

For Household Burglary-Only Installations: The total current drawn from the alarm output may be up to 1.7A. A battery must be installed to supply the current of the combined auxiliary power, polling loop, and alarm output in excess of 750mA.

Failure to observe the polling loop current rating will cause polling loop malfunction. Failure to observe the auxiliary power current rating will result in a battery that does not charge properly or possibly a tripped circuit breaker.

To connect the transformer to the control, perform the following steps:

Step	Action
1	Connect all installed devices to the control.
2	Wire the 1361 Transformer (1361CN in Canada) to the panel (before connecting the battery) as shown in *Figure 3-27*, or wire the 1361X10 Transformer as shown in *Figure 3-28* (if using X-10 devices).
3	Plug the transformer into a 24-hour, uninterrupted, 120VAC, 60Hz outlet. After a few seconds, the keypad display appears.

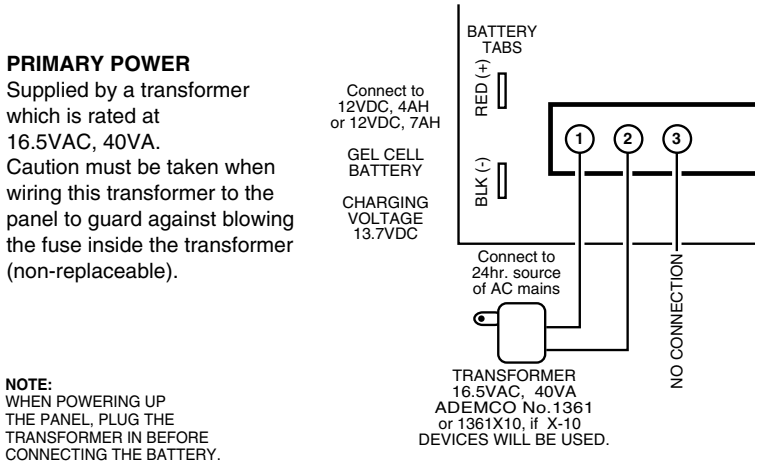


Figure 3-27: 1361 Transformer and Battery Connections

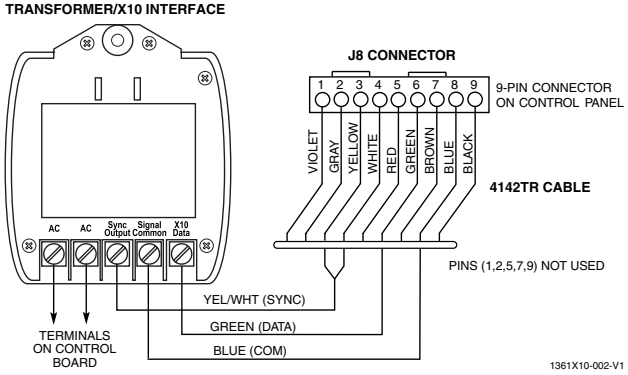


Figure 3-28: 1361X10 Transformer Connections

Panel Earth Ground Connections

In order for the lightning transient protective devices in this product to be effective, the designated earth ground terminal (terminal 30) must be terminated in a good earth ground. Recommended wire gauge for the ground connection is #16 AWG, run no farther than 30 feet. The following are examples of good earth grounds available at most installations:

- **Metal Cold Water Pipe:** Use a noncorrosive metal strap (copper is recommended) firmly secured to the pipe to which the ground lead is electrically connected and secured.
-
- **AC Power Outlet Ground:** Available from 3-prong, 120VAC, power outlets only. To test the integrity of the ground terminal, use a three-wire circuit tester with neon lamp indicators, such as the UL-Listed Ideal Model 61-035, or equivalent, available at most electrical supply stores.

The panel requires the earth ground connection for its lightning transient protection devices.

Determining the Control's Power Supply Load

Use the tables that follow to calculate the total current for the Auxiliary Power, the Alarm Output, and the Polling Loop. In each table, multiply each device's standby and/or alarm current by the number of units used.

1. In Table 1, enter devices used on the polling loop. Calculate total current draw on the polling loop.

Table 1: Total Polling Loop Current Draw

Polling Loop Device	Current	# of Units	Total
Polling Loop Subtotal (terminals 24 & 25 – 128mA) ✳			

✳ The total current cannot exceed 128mA. If total load exceeds 128mA, then a 4297 Loop Extender Module can be used. Note that the total number of points connected to the panel cannot exceed 119.

2. In Table 2, enter devices used on Auxiliary Power. Calculate standby and alarm currents, then add to get Auxiliary Power current subtotal.

Table 2: Auxiliary Power Current Load

Device Model #	Device Current X # of Units		Total Current	
			Standby	Alarm
Auxiliary Power Subtotal (terminals 6 & 7 – 750mA max.)				

3. In Table 3, enter devices connected to the Alarm Output. Calculate alarm currents, then add to get the Alarm Output current subtotal.

Table 3: Alarm Output Current Load

Device Model #	Device Current X # of Units		Total Current	
			Standby	Alarm
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
			XXXXXX	
Alarm Output Subtotal (terminals 4 & 5 – 1.7A max.)				

4. In Table 4, enter the total calculated subtotals of all listed outputs from Tables 1 through 3, then add to get the combined current.

Table 4: Total VISTA-128BPT/VISTA-250BPT Current Load

	Total Current	
	Standby	**Alarm**
Polling Loop Subtotal (see Table 1)		
Aux. Power Subtotal (see Table 2)		
Alarm Output Subtotal (see Table 3)		
VISTA-128BPT/VISTA-250BPT PCB Current (Includes 2-wire smoke detector loading on zone 1)	250mA	330mA
Total Current Load		

Determining the Size of the Standby Battery

The cabinet supplied with the control panel can house batteries of up to 12V, 14AH (two 12V, 7AH batteries wired in parallel). The VISTA-ULKT kit provides a cabinet that can house batteries of up to 12V, 17.2AH and that may be used with this panel. The total standby current drawn from the auxiliary power and polling loop outputs combined must be limited to 270mA when 14AH batteries are used; and to 390mA when 17.2AH batteries are used.

DO NOT use Gates batteries (sealed lead-acid type). These batteries require a different charging voltage than is supplied by the panel.

UL The maximum battery capacity in UL installations is 14AH.

UL Household Fire or Combination Household/Fire/Burglary installations require the use of a backup battery that is capable of providing 24 hours of standby time followed by 4 minutes of alarm time. UL1023 Household Burglary-only installations require the use of a backup battery that is capable of providing 4 hours of standby time followed by 4 minutes of alarm time.

Use Table 5 to determine the required backup battery capacity and use Table 6 to determine the battery model number. **A dual battery harness is supplied** that allows two batteries to be wired in parallel for increased capacity.

5. Using the total calculated from Table 4, calculate the battery capacity required for the installation.

Table 5: Battery Capacity Calculation Table

Capacity	Formula	Calculated Value
Standby Capacity	For 4-hour standby time: Total **standby current** X 4 hours X 1.4 contingency factor. For 24-hour standby time: Total **standby current** X 24 hours X 1.1 contingency factor.	
Alarm Capacity	For 4-, 5-, or 15-minute alarm time: Total **alarm curr.** X 0.067 (4 min) 0.250 (15 min)	
Total Capacity	**Add standby and alarm capacities**	

6. Use the Battery Selection Table to select the appropriate battery for the installation.

Table 6: Battery Selection Table

Capacity	Recommended Battery	Comment
4AH	Yuasa NP4-12	
7AH	Yuasa NP7-12	
12AH	Yuasa NP12-12	Fits in large mercantile cabinet only.
14AH	Yuasa NP7-12	Connect two in parallel.
17.2AH	Yuasa NPG18-12	Fits in large mercantile cabinet only.

The standby battery is automatically tested for 10 minutes every 4 hours, beginning 4 hours after exiting Programming mode. In addition, entry into the Test mode initiates a battery test. The VISTA-128BPT/VISTA-250BPT also runs a 5-second battery test every 60 seconds to check if the battery is connected.

7. Connect the battery, referring to *Figure 3-27*.

Programming

NOTE: All references in this manual for number of zones, number of user codes, number of access cards, and the dialer queue capacity, use the VISTA-250BPT's features. See *SECTION 1: General Description* for the table listing the differences between the VISTA-128BPT and the VISTA-250BPT control panels.

Program Modes

There are two programming modes for the VISTA-128BPT/VISTA-250BPT. These are the Data Field Program Mode and the #93 Menu Mode. The Data Field Program Mode is where many system options are programmed. The #93 Menu Mode is an interactive mode that requires a 2-line alpha keypad (6160).

The factory-loaded defaults (✳97) enable keypad addresses 00-01 only. A keypad set to one of these addresses must be used to program the system initially.

Local keypad programming can be disabled through Compass downloading software. If this is done, Program mode can only be accessed via the downloading software.

Entering and Exiting Programming Mode

Enter Programming mode using either method a or b:

a. Press both the [✳] and [#] keys at the same time within 30 seconds after power is applied to the control.

b. Enter the **Installer Code + [8] + [0] + [0] + [0]** keys. The factory installer code can be changed once in the Program mode (field ✳00).

NOTE: The default for the Installer Code is 4140.

Exit the Programming mode by either method a or b:

a. Press [✳] + **[9]** + **[8]**. Exiting by this method prevents the installer code from being used to re-enter Programming mode. Only method "a" can be used to re-enter Programming mode.

b. Press [✳] + **[9]** + **[9]**. Exiting by this method permits the installer code to be being used to re-enter Programming mode.

Data Field Programming Mode

In the Data Field Program Mode you may access any field simply by entering either [✳] or [#] + the field number:

- To write or change information in a field press [✳] + the field number (✳03).
- To read the information in a field press [#] + the field number (#03).

When the entries for a field are completed, the keypad beeps three times and advances to the next field.

Summary of Data Field Programming Commands

✳**91**	Select partition for programming partition-specific fields
✳**92**	Display the software revision level of the control panel
✳**93**	Enter Menu mode programming
✳**94**	Go to next page of fields
✳**99**	Go back to previous page of fields or exit Programming Mode with no installer code lockout
✳**98**	Exit Programming Mode with Installer Code lockout

Moving Between Programming Levels

The data fields are grouped into three levels (referred to as "pages"). The first page is accessed as soon as Programming Mode is entered.

The second and third pages of data fields are indicated at the keypad by a 1 and 2, respectively, in front of the 2-digit field address. "ALT PROGRAM MODE" is displayed along with a "100" or "200," indicating which page of program fields is accessed.

To access the next level of programming fields, perform the following steps:

Step	Action
1	Press ✳94.
2	Press [✳] + [XX], where XX = the last two digits of the program field, and make the desired entry.

NOTES:

Press ✳94 to move to 2nd page, (fields 1✳01 - 1✳76); press ✳99 to move back to 1st page.

Press ✳94 to move to 3rd page (fields 2✳00 - 2✳88); press ✳99 to move back to 2nd page

Entry Errors

- If an address is improperly entered, the keypad displays "FC."
- If a program entry is improperly entered (for example, a larger number than is permitted), the keypad display will go blank.

In either of the above cases, simply re-enter [✳] + the correct field number and then enter the correct data.

Programming System-Wide Data Fields

Values for some programming fields are system-wide (global), and some can be different for each partition (partition-specific).

The partition-specific programming fields are automatically skipped when programming the global fields. If the system has only 1 partition, the partition-specific fields *are not* automatically skipped.

To program system-wide data fields, perform the following steps:

Step	Action
1	Enter Program Mode: **Installer Code + 8 0 0 0.** The following display appears: Program Mode ✳Fill # View – 00
2	If the control has not been programmed before, enter ✳97 to load factory defaults**.**
3	Press [✳] and enter the first field number to be programmed (for example, ✳00, Installers Code). Make the desired entry. When the field is complete, the keypad beeps three times and advances to the next field. If you do not want to change the next field, press [✳] and enter the next field number to be programmed. First Page of fields (✳00 - ✳90) To change to the next page of fields, press ✳94. To return to the previous page of fields, press ✳99.
4	Press ✳99 or ✳98 to exit Program Mode.

NOTE: If the number of digits that you enter in a data field is fewer than the maximum permitted (for example, a phone number), the keypad displays the last entry and waits. To proceed, enter [✳] + the next data field you wish to program.

Programming Partition-Specific Data Fields

To program partition-specific data fields once in Program Mode, do the following:

Step	Action
1	Enter Program Mode: **Installer Code + 8 0 0 0.**
2	Press ✳91, which will prompt you for the partition number desired.
3	Enter a partition-specific field number (e.g., ✳09) to begin programming. When the first field's entry is completed, the next partition-specific field is automatically displayed. When all partition-specific fields are programmed, the system returns to the global programming fields (page 1 fields).
4	Repeat this procedure for each partition in the installation.

NOTE: To return to the global program fields before finishing all fields, enter any global field number.

Programming Partition-Specific Fields

Press ✳91 to select a partition.
↓
Enter the partition to be programmed.
↓
Enter a partition-specific field number and make entry.
↓
After partition-specific fields are programmed, press ✳91 to select next partition.

Enter any global field number to return to the global fields at any time.

#93 Menu Mode Programming

The #93 Menu Mode is an interactive mode through which much of the system's programming is done. In this mode, there are "question and answer" prompts that can be accessed once Data Field Program Mode has been entered. These prompts require a 2-line alpha keypad (6160).

After programming all system-related programming fields in the usual way, press #93 while still in programming mode to display the first choice of the menu-driven programming functions. Press 0 (NO) or 1 (YES) in response to the displayed menu selection. Pressing 0 will display the next choice in sequence.

Below is a list of the main menus. For details refer to the *VISTA-128BPT/VISTA-250BPT Programming Guide*.

MAIN MENU	OPTIONS
ZONE PROG? 1 = YES 0 = NO 0	For programming the following: • Zone Number • Zone Response Type • Partition Number for Zone • Dialer report code for zone • Input Device Type for zone (whether RF, polling loop, etc.) • Enrolling serial numbers of 5800 Series transmitters & serial polling loop devices into the system. • Zone Attributes (e.g., Arm w/Fault, Silent, etc.).
EXPERT MODE? 1 = YES 0 = NO 0	Same as Zone Programming except: • Done with a minimum number of keystrokes. • Can program wireless keys using pre-defined templates.
REPORT CODE PROG? 1 = YES 0 = NO 0	For programming the following: • Alarm report codes for zones • Restore and supervisory codes • All other system report codes
ALPHA PROG? 1 = YES 0 = NO 0	For entering alpha descriptors for the following: • Zone Descriptors • Installer's Message • Custom Words • Partition Descriptors • Relay Descriptors
DEVICE PROG? 1 = YES 0 = NO 0	For defining the following device characteristics for addressable devices, including keypads, RF receivers (5881), output relay modules (4204), 4286 VIP Module, and ECP Communicators (7845i-ent, 7845GSM, 7845i-GSM, etc.): • Device Address • Device Type • Keypad Options (including Partition assignment) • RF House ID • LRR Options (including Programming radio)
OUTPUT PGM? 1 = YES 0 = NO 0	For defining output device functions.
RLY VOICE DESCR? 1 = YES 0 = NO 0	For entering voice descriptors for relays to be used with the 4286 VIP Module.
CUSTOM INDEX ? 1 = YES 0 = NO 0	For creating custom word substitutes for VIP Module annunciation.
ACCESS POINT PGM 1 = YES 0 = NO 0	For defining the parameters for each of the VistaKey zones, including which group(s) have access through an access point (door). See the *VistaKey-SK Installation and Setup Guide* for detailed programming instructions.
ACCESS GRP PGM 1 = YES 0 = NO 0	For defining the capabilities (privileges) for each group of users. See the *VistaKey-SK Installation and Setup Guide* for detailed programming instructions.
EVENT/ACTION PGM 1 = YES 0 = NO 0	For defining events and time windows for an access group. See the *VistaKey-SK Installation and Setup Guide* for detailed programming instructions.

Following is a list of commands used while in the Menu Mode:

#93 Menu Mode Programming Commands

#93	Enters Menu Mode.
[✳]	Serves as [ENTER] key. Press to have keypad accept entry.
[#]	Backs up to previous screen.
0	Press to answer NO.
1	Press to answer YES.
00, or 000+[✳]	Quits Menu Mode and goes back to Data Field Programming Mode, if entered at first prompt of each main menu option.

Zone Number Designations

The VISTA-128BPT supports up to 128 zones, the VISTA-250BPT supports up to 250 zones, of hardwire, polling loop and/or wireless protection, distributed among up to eight partitions. The following table lists the zone numbers and the types of sensors that can be used with each, and some alternate functions of the zones.

Zone	Function
1	2-wire Smoke Detectors (if used)
5	Audio Alarm Verification (if used)
7	Keyswitch (if used)
1-9	Traditional Hardwired Zones
9	For unsupervised, N.C. use only.
1-250	5800 Series Wireless Devices
10-250	Polling Loop Devices
995	✳ + 1 Panic
996	# + 3 Panic
999	✳ + # Panic

Zone Defaults

Zone #	Zone Type	Zone #	Zone Type
001	09	601-632	00
002	03	800-830	00
003	03	970	00
004**	04	988	00
005	03	990	00
006	03	992*	N/A
007	03	995	00
008	03	996	00
009	03	997	05
010–250	00	999	06

NOTES:

* Zone 992 is the Duress zone. Programming of the zone response type is not applicable. This zone requires only the report code programming.

**Zone 004 is also defaulted with Auto-STAY enabled.

Zone Index

The zones are designated as follows:

ZONE # RANGE	ZONE FUNCTION	ACTUAL ZONE
001 – 250	Protection zones	As indicated
601 – 632	Relay Supervisory Zones	6 + 2-digit Relay Number; e.g., Relay Number 03 is zone 603.
800 – 830	ECP Device Supervisory Zones	8 + 2-digit Device Address; e.g., Device Address 01 is zone 801. VIP Module is zone 804 (Device Address must be set to 4).
970, 988, 990, & 997	System Supervisory Zones	970: Bell Supervision 988: 2nd Wireless Receiver – not receiving signals 990: 1st Wireless Receiver – not receiving signals 997: Polling Loop (short circuit)
992, 995 – 999	Duress and Keypad Panics	992: Duress 995: 1 + ✳ panic (A key) 996: 3 + # panic (C key) 999: ✳ + # panic (B key)

Program supervisory zones with response type of 05.

Communication Defaults

*45	PRIMARY FORMAT	[1] ADEMCO Contact ID
*47	SECONDARY FORMAT	[1] ADEMCO Contact ID
*51	DUAL REPORTING	[0] no

Communication Defaults for Zones

ZONE #	1st	2nd	ZONE #	1st	2nd	ZONE #	1st	2nd	ZONE #	1st	2nd
1	01	00	**50**	05	00	**99**	09	00	**148**	13	00
2	02	00	**51**	06	00	**100**	10	00	**149**	14	00
3	03	00	**52**	07	00	**101**	11	00	**150**	15	00
4	04	00	**53**	08	00	**102**	12	00	**151**	01	00
5	05	00	**54**	09	00	**103**	13	00	**152**	02	00
6	06	00	**55**	10	00	**104**	14	00	**153**	03	00
7	07	00	**56**	11	00	**105**	15	00	**154**	04	00
8	08	00	**57**	12	00	**106**	01	00	**155**	05	00
9	09	00	**58**	13	00	**107**	02	00	**156**	06	00
10	10	00	**59**	14	00	**108**	03	00	**157**	07	00
11	11	00	**60**	15	00	**109**	04	00	**158**	08	00
12	12	00	**61**	01	00	**110**	05	00	**159**	09	00
13	13	00	**62**	02	00	**111**	06	00	**160**	10	00
14	14	00	**63**	03	00	**112**	07	00	**161**	11	00
15	15	00	**64**	04	00	**113**	08	00	**162**	12	00
16	01	00	**65**	05	00	**114**	09	00	**163**	13	00
17	02	00	**66**	06	00	**115**	10	00	**164**	14	00
18	03	00	**67**	07	00	**116**	11	00	**165**	15	00
19	04	00	**68**	08	00	**117**	12	00	**166**	01	00
20	05	00	**69**	09	00	**118**	13	00	**167**	02	00
21	06	00	**70**	10	00	**119**	14	00	**168**	03	00
22	07	00	**71**	11	00	**120**	15	00	**169**	04	00
23	08	00	**72**	12	00	**121**	01	00	**170**	05	00
24	09	00	**73**	13	00	**122**	02	00	**171**	06	00
25	10	00	**74**	14	00	**123**	03	00	**172**	07	00
26	11	00	**75**	15	00	**124**	04	00	**173**	08	00
27	12	00	**76**	01	00	**125**	05	00	**174**	09	00
28	13	00	**77**	02	00	**126**	06	00	**175**	10	00
29	14	00	**78**	03	00	**127**	07	00	**176**	11	00
30	15	00	**79**	04	00	**128**	08	00	**177**	12	00
31	01	00	**80**	05	00	**129**	09	00	**178**	13	00
32	02	00	**81**	06	00	**130**	10	00	**179**	14	00
33	03	00	**82**	07	00	**131**	11	00	**180**	15	00
34	04	00	**83**	08	00	**132**	12	00	**181**	01	00
35	05	00	**84**	09	00	**133**	13	00	**182**	02	00
36	06	00	**85**	10	00	**134**	14	00	**183**	03	00
37	07	00	**86**	11	00	**135**	15	00	**184**	04	00
38	08	00	**87**	12	00	**136**	01	00	**185**	05	00
39	09	00	**88**	13	00	**137**	02	00	**186**	06	00
40	10	00	**89**	14	00	**138**	03	00	**187**	07	00
41	11	00	**90**	15	00	**139**	04	00	**188**	08	00
42	12	00	**91**	01	00	**140**	05	00	**189**	09	00
43	13	00	**92**	02	00	**141**	06	00	**190**	10	00
44	14	00	**93**	03	00	**142**	07	00	**191**	11	00
45	15	00	**94**	04	00	**143**	08	00	**192**	12	00
46	01	00	**95**	05	00	**144**	09	00	**193**	13	00
47	02	00	**96**	06	00	**145**	10	00	**194**	14	00
48	03	00	**97**	07	00	**146**	11	00	**195**	15	00
49	04	00	**98**	08	00	**147**	12	00	**196**	01	00
197	02	00	**215**	05	00	**232**	07	00	**249**	09	00
198	03	00	**216**	06	00	**233**	08	00	**250**	10	00
199	04	00	**217**	07	00	**234**	09	00	**601-632**	00	00
200	05	00	**218**	08	00	**235**	10	00	**800-830**	00	00
201	06	00	**219**	09	00	**236**	11	00	**970**	00	00
202	07	00	**220**	10	00	**237**	12	00	**988**	00	00
203	08	00	**221**	11	00	**238**	13	00	**990**	00	00
204	09	00	**222**	12	00	**239**	14	00	**992 (DURESS)**	11	00
205	10	00	**223**	13	00	**240**	15	00	**995**	00	00
206	11	00	**224**	14	00	**241**	01	00	**996**	00	00
207	12	00	**225**	15	00	**242**	02	00	**997**	06	00
208	13	00	**226**	01	00	**243**	03	00	**999**	06	00
209	14	00	**227**	02	00	**244**	04	00	**ALARM RST.**	00	00
210	15	00	**228**	03	00	**245**	05	00	**TROUBLE**	00	00
211	01	00	**229**	04	00	**246**	06	00	**TRBLE. RST**	00	00
212	02	00	**230**	05	00	**247**	07	00	**BYPASS**	00	00
213	03	00	**231**	06	00	**248**	08	00	**BYP. RST.**	00	00
214	04	00									

Zone Response Type Definitions

Each zone must be assigned a zone type, which defines the way in which the system responds to faults in that zone. There are three keypad-activated zones (panic keys; see note) for each partition, a polling loop supervision zone, and four RF supervisory zones, two for each RF receiver installed. Zone types are defined below.

Type 00: Zone Not Used

Program with this zone type if the zone is not used.

Type 01: Entry/Exit #1 Burglary

Provides entry delay whenever the zone is faulted and the system is armed in the AWAY or STAY mode. When the panel is armed in the INSTANT or MAXIMUM mode, no entry delay is provided. Exit delay begins whenever the control is armed, regardless of the arming mode selected. These delays are programmable.

Assign this zone type to zones that are used for primary entry to and exit from the facility.

Type 02: Entry/Exit #2 Burglary

Provides a secondary entry delay, if the system is armed in the AWAY or STAY modes and the zone is faulted. When the panel is armed in the INSTANT or MAXIMUM mode, no entry delay is provided. Secondary exit delay begins whenever the control is armed, regardless of the arming mode selected. These delays are programmable.

Assign this zone type to zones that are used for entry and exit of the facility and require more time than the primary entry and exit point. Delay times for this zone type must be greater than those for zone type 01 (e.g., a garage, loading dock, or basement door).

Type 03: Perimeter Burglary

Provides an instant alarm if the zone is faulted and the system is armed in the AWAY, STAY, INSTANT, or MAXIMUM mode.

Assign this zone type to all exterior door and window zones.

Type 04: Interior, Follower

Provides a delayed alarm (using the programmed entry delay time) if an entry/exit zone is faulted first. Otherwise it produces an instant alarm. It is active when the system is armed in the AWAY or MAXIMUM mode, but the MAXIMUM mode eliminates the entry delay.

If the Interior Follower zone is programmed for one of the STAY modes (default is STAY mode 1), it is automatically bypassed when the panel is armed in the STAY or INSTANT mode.

Assign this zone type to a zone covering an area such as a foyer, lobby, or hallway through which one must pass upon entry or exit (to and from the keypad).

Type 05: Trouble by Day/Alarm by Night

Provides an instant alarm if the zone is faulted and the system is armed in the AWAY, STAY, INSTANT, or MAXIMUM mode. During the disarmed state (day), the system annunciates a latched trouble sounding from the keypad (and a central station report, if desired).

Assign this zone type to a zone that contains a foil-protected door or window (such as in a store), or to a zone covering a sensitive area such as a stock room or drug supply room. It can also be used on a zone in an area where immediate notification of an entry is desired.

Type 06: 24-Hour Silent Alarm

Sends a report to the central station but provides no keypad display or sounding. Assign this zone type to a zone containing an Emergency button.

Type 07: 24-Hour Audible Alarm

Sends a report to the central station and provides an alarm sound at the keypad and an audible external alarm. Assign this zone type to a zone containing an Emergency button.

Type 08: 24-Hour Auxiliary Alarm

Sends a report to central station and provides an alarm sound at the keypad only. **(No bell output is provided.)** Assign this zone type to a zone an Emergency button or one containing monitoring devices such as water sensors or temperature sensors.

Type 09: Supervised Fire (Without Verification)

Provides a fire alarm on a short circuit and a trouble condition on open circuit. A fire alarm produces a pulsing of the bell output. A zone of this type is always active and cannot be bypassed.

Type 10: Interior with Delay

Provides entry and exit delays (using the programmed entry and exit delay times) when armed in the AWAY mode. Provides only exit delay when armed in the MAXIMUM mode (no entry delay).

If the Interior with Delay zone is programmed for one of the STAY modes (default is STAY mode 1), it is automatically bypassed when the panel is armed in the STAY or INSTANT mode. Delay begins whenever sensors in this zone are violated, regardless of whether or not an entry/exit delay zone was tripped first.

Assign this zone type to a zone covering an area such as a foyer, lobby, or hallway through which one must pass upon entry or exit (to and from the keypad).

Type 12: Not Used

Type 14: CO Detector Alarm

Sends a report to the central station and displays a CO text message at the keyboard. Upon a CO alarm only the keypad's sounder will annunciate. The external bell will not sound at all. A zone of this type is always active and cannot be bypassed.

Type 16: Fire With Verification

Provides a fire alarm on a short circuit and a trouble condition on open circuit. An initial short detection causes 7-second smoke detector power reset. A subsequent short detection within 90 seconds of the reset causes a fire alarm. A fire alarm produces a pulsing of the bell output. A zone of this type is always active and cannot be bypassed.

Type 20: Arm-STAY (5800 Series devices only)

Causes the system to arm in the STAY mode when the zone is activated.

Type 21: Arm-AWAY (5800 Series devices only)

Causes the system to arm in the AWAY mode when the zone is activated.

Type 22: Disarm (5800 Series devices only)

Causes the system to disarm when the zone is activated.

Type 23: No Alarm Response

Used on a zone when an output relay action is desired, but with no accompanying alarm (e.g., for lobby door access).

Type 27: Access Point

Assign this zone type to an input device (hardwired zone, wireless zone, keypad, access control relay, etc.) that controls an access entry point (e.g., a door). The access point entry relay can be assigned to an access control relay (controlled by the VISTA-128BPT/VISTA-250BPT), ECP relay (4204), or to the access control system independent of the control panel.

Type 28: Not Used.

Type 29: Momentary Exit

Used to cause an access point programmed for entry to revert to an exit point for 15 seconds. After the 15 seconds, it automatically reverts to an entry point. This zone type should be used only with VistaKey modules.

NOTE FOR PANIC KEYS: Keypad panic zones share the same zone response type for all eight partitions, but panics may be individually enabled for each partition.

IMPORTANT! FAULT ANNUNCIATION

Polling loop and RF troubles (zones 988, 990, and 997) report as trouble conditions only, and as such, should be assigned zone type 05 if annunciation is desired. See *Polling Loop Supervision* and *RF System Operation and Supervision* in *SECTION 3 Installing the Control* for more information.

Zone Input Type Definitions

Each zone must be assigned an input type, which defines the where the system will "look" for status of the zone (RF receiver, polling loop, etc.). Zone input types are defined below.

Type 01 Hardwired (HW)

Reserved for the built-in hardwired zones 1-9.

Type 02 RF Motion (RM)

Select for 5800 Series RF transmitters. Sends periodic check-in signals, as well as fault and low-battery signals. The control panel automatically restores the zone to "ready" after a few seconds. This type is designed for facilities with multiple motion detectors that may fault and restore simultaneously. The transmitter must remain within the receiver's range. **NOTE:** If using RF Motion with a door/window type transmitter, only loop 1 may be used.

Type 03 Supervised RF (RF)

Select for 5800 Series RF transmitters that will be supervised for check-in signals. The transmitter must remain within the receiver's range.

Type 04 Unsupervised RF (UR)

Select for 5800 Series RF transmitters that will not be supervised for check-in signals. The transmitter may therefore be carried off-premises.

Type 05 Unsupervised Button RF (BR)

Select for 5800 Series RF transmitters specifically designed for this input type. Check the transmitter's instructions for proper programming of the input type. These transmitters send only fault signals. They do not send low-battery signals until they are activated. The transmitter may be carried off-premises.

Type 06 Serial Number Polling Loop (SL)

Select for polling loop devices with a built-in serial number.

For VistaKey, select this type for Door Status Monitor Backup DSMB. If local power to the VistaKey is lost, a V-Plex SIM, located on the VistaKey board, is powered directly from the polling loop and reports the state of the DSM via the standard V-Plex polling system.

NOTE: To obtain the DSMB function, the Input Type must be defined as 06 and the next prompt in Zone Programming (Access Point) must contain the Access Point number (01-15) (address of the VistaKey module).

Type 07 DIP Switch Loop (DP)

Select for polling loop devices that use DIP switches for programming the zone number of the device.

Type 08 Dip Switch Polling Loop Right Loop (PS)

Select for the second loop of two-zone polling loop devices (e.g., 4190WH; 4278).

Type 09 Console Input (CS)

Select when this zone is to be controlled by a keypad input (user code + [#] + [7] + [3]) for access control.

Type 10 Not Used

Type11 VistaKey Door Status Monitor (DSM)

Select this input type when using a VistaKey module connected to a door. This must be programmed for each VistaKey module to provide the DSM zone mapping a panel zone. If this is not programmed the panel will not "see" the VistaKey module.

It is also used to determine the door is opened after a card swipe or if the door is being held open. The device is normally a magnetic switch mounted on the door. The status of the switch is different when the door is in an open position.

Type 12 VistaKey Request to Exit (RTE)

Use this input type to map an uncommitted RTE zone to an alarm panel zone. This input type is not normally used if the zone is used for a request-to-exit function.

Type 13 VistaKey General Purpose (GP)

This input type operates in the same manner as other VISTA-128BPT/VISTA-250BPT alarm panel zones and is provided so that a zone in the proximity of the VistaKey can be wired without having to run additional wiring from the control panel.

.

Programming for Access Control

VistaKey

See the *VistaKey-SK Installation and Setup Guide* for the detailed programming instructions.

VistaKey Dialer Enables

When the VistaKey is installed with an alarm system, the system defaults are set so that the system does not send reports to the central station. The programming is accomplished in field 1∗35 for the following events:

- ACS Troubles - To enable or disable ACS trouble reporting.
- ACS Bypasses - To enable or disable ACS bypass reporting.
- ACS System - To enable or disable ACS system reporting, (i.e., ACS module reset).
- ACS Alarms - To enable or disable ACS alarm reporting.
- Dialer (Trace) - To enable or disable access grant/denial events sent to the central station.

Access Control of an Entry/Exit Point

The control can send entry and exit requests to the VistaKey ACS utilizing keypads and button-type (BR) RF transmitters. A zone is programmed with a response type 27 (Access Point) and an appropriate input type (console, RF).

Using the Alpha Keypad

Step	Action
1	Enter Zone Programming in the #93 Menu Mode.
2	Program the zone with a response type 27 (Access Point).
3	Enter the access point number (00-31) of the door.
4	Program whether this is an entry or exit point.
5	Enter the partition number.
6	Enter the input type as CS (09).
7	Enter the keypad ECP address.

See Zone Programming in the Programming Guide for a detailed explanation.

Using Wireless Keypads

UL Wireless Keypads 5827 and 5827BD are not UL Listed and are not suitable for use in a UL installation.

Wireless keypads (5827 & 5827BD) can provide another way of entering or exiting the premises. They function the same as alpha keypads, except when the code + # 73 is entered. This entry will allow momentary access to ALL access points in the partition to which the keypad is assigned. To program the wireless keypad, enter the partition the keypad is assigned to in field 1*48.

Using an RF Transmitter Zone

A button type RF transmitter (5804) can be used to provide access or egress for up to 4 doors. One button will control one door. Also, a button can be used to provide access or egress due to a panic or duress condition.

To program the RF transmitter for access control, perform the following steps:

Step	Action
1	Enter Zone Programming in the #93 Menu Mode.
2	Program the zone with a response type 27 (Access Point).
3	Enter the access point number (00-31) of the door.
4	Indicate whether RF device is for entry or exit.
5	Enter the partition number
6	Enter the input type: button RF (03).
7	Enter the loop number.
8	Enroll the serial number

See Zone Programming in the Programming Guide for a detailed explanation.

- RF buttons and pendants must be assigned to a user number in order to function. See *SECTION 9: User Access Codes* for the procedure.
- An RF transmitter will not provide access or grant if the system is in any test mode.

Control of Lighting and Appliances

Lighting and appliances can be controlled when an access or exit event occurs. Lights or appliances can be automatically turned on or off when a valid entry or egress request is presented at an access point. To control these devices, the VISTA-128BPT/VISTA-250BPT relays or the ACS relays or triggers are used with keypads and/or RF transmitters whose response type is Access Point (27). To program the control of lighting and appliances, perform the following steps:

Step	Action
1	Enter Output Programming in the #93 Menu Mode.
2	Program all the information for the relay.
3	Select the output type: ECP (1) (4204) or (2) (X-10).

See Output Programming in the Programming Guide for a detailed explanation.

Using the VISTA-128BPT/VISTA-250BPT for Stand-Alone Access Control

The VISTA-128BPT/VISTA-250BPT can be used for access control without interfacing to VistaKey. A user can trigger an access point (i.e., door strike) for 2 seconds by entering User Code + [0]. To program the VISTA-128BPT/VISTA-250BPT for Stand-Alone access control, perform the following steps:

Step	Action
1	Enter Output Programming in the #93 Menu Mode.
2	Program the output type as 1, or 2.
3	For type 1, program the ECP address and relay number.
4	For type 2, program the house and unit codes.
5	Program the relay number in field 1∗76 (partition-specific).

See Output Programming in the Programming Guide for a detailed explanation.

Programming for ECP Communicator

- Program the Communicator in *Device Programming* in the #*93 Menu Mode Programming*.
- Field ∗56: Selects the time the panel should wait before it attempts to send a message to the second destination.
- Field ∗57: Select the initial reporting destination for messages.
- Field ∗58: Select events for the primary sub's ID
- Field ∗59: Select events for the secondary sub's ID.

Data Field Descriptions

About Data Field Programming

The following pages list this control's data fields in numerical order. Field numbers are listed in the left column, followed by a "Title and Data Entries column, which lists the valid entries for each field. Experienced installers can simply follow this column when programming the data fields. The "Explanation" column provides explanatory information and special notes where applicable.

NOTE: Refer to the *Programming Guide* for the default values. They are not listed in this section.

Use the *Programming Guide* to record the data for this installation.

NOTE: All references in this manual for number of zones, number of user codes, number of access cards, and the event log capacity, use the VISTA-250BPT's features. See *SECTION 1: General Description* for the table listing the differences between the VISTA-128BPT and the VISTA-250BPT control panels. All other features are identical, except for the Remote Keypad Sounder (field 1✳46 option 2), which is available only in the VISTA-128BPT.

Programming Data Fields

Data field programming involves making the appropriate entries for each of the data fields. Start Data Field programming by entering the installer code + 8 + 0 + 0 + 0.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***00**	**Installer Code** Enter 4 digits, **0-9**	The Installer Code is a 4-digit code reserved for installation company use. This is the only code that can be used to enter the Program Mode from the keypad. This code cannot be used to disarm the system if it isn't used to arm the system. This code cannot be used to re-enter Program Mode if Program Mode is exited by the *98 command.
***04**	**Enable Random Timers For Partitions 1-8** **0** = disable **1** = enable	If enabled, the activation time of the window is randomized up to 30 minutes and is initialized by either of two methods: **User Code** + **[#]** + **[41]**Initiates the random schedule for all devices in the partition. **User Code** + **[#]** + **[42]**Initiates the random schedule for all devices in the partition with a time window within 6 PM and 5 AM.
***05**	**System Events Notify** **0** = disable **1** = enable	If enabled the system sends notification messages via the RS232 port (TB4). Field *14 must be set for RS232 port **(1)**. **NOTE:** If enabled, the system also sends fault and restore messages via the RS232 port (TB4). **NOTE:** While in a communication session with Compass, system events will not operate.
***06**	**Quick Exit (partition-specific)** **0** = disable **1** = enable	If enabled, allows users to exit the armed partition without disarming and then rearming the partition. Quick Exit is initiated by entering [#] + [9]. This restarts the exit delay. All rules of exit apply, including exit error logic.

UL Quick Exit is not permitted for use with the VISTA-128BPT/VISTA-250BPT Control Panel in a UL installation.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***09**	**Entry Delay #1 (partition-specific)** Enter **02-15** multiplied by 15 seconds. **00** = no delay.	Entry delay defines the delay time that allows users to re-enter the premises through a door that has been programmed as an entry delay door and disarm the system without sounding an alarm. The system must be disarmed within this period or an alarm will occur. **NOTE:** The delay may not exceed 45 seconds for UL installations.
***10**	**Exit Delay #1 (partition-specific)** Enter **02-15** multiplied by 15 seconds. **00** = no delay.	Exit delay defines the delay period that allows users to leave the premises through a door that has been programmed as an entry/exit delay door after arming the system without setting off the alarm.
***11**	**Entry Delay #2 (partition-specific)** Enter **02-15** multiplied by 15 seconds. **00** = no delay.	Entry Delay #2 is used for a secondary door requiring a longer delay than those assigned to Entry Delay #1. **NOTE:** The delay may not exceed 45 seconds for UL installations.
***12**	**Exit Delay #2 (partition-specific)** Enter **02-15** multiplied by 15 seconds. **00** = no delay.	Exit Delay #2 is used for a secondary door requiring a longer delay than those assigned to Exit Delay #1. **NOTE:** The delay may not exceed 60 seconds for UL installations.
***13**	**Alarm Sounder Duration (Bell Timeout) (partition-specific)** Enter **01-15** multiplied by 2 minutes.	Defines the length of time the Bell Output and the keypad's sounder will sound for all audible alarms. Must be minimum 16 minutes for UL Commercial Burglary installations.
***14**	**RS232 Input** **0** = Disable **1** = Enable	When enabled, sets RS232 input at TB4.
	UL Using the RS232 input (TB4) for automation is not permitted in UL installations.	
***15**	**Keyswitch Assignment** Enter **1-8** partition keyswitch is being used. Enter **0** if the keyswitch is not used.	The keyswitch requires the use of zone 7 wired loop (zone 7 is no longer available as protection zone). The fire and panic alarm voltage triggers (J7) automatically become ARMING and READY status outputs for the Keyswitch LEDs. Openings/closing report as user "0" if enabled in field *40.
***16**	**Confirmation of Arming Ding (partition-specific)** **0** = disable **1** = enable	If enabled, produces ½-second external alarm sounding ("ding") at the end of exit delay (or after kissoff from the central station, if sending closing reports). **NOTE:** If using a keyfob, when the button is pressed, either for arming or disarming, the bell will ding indicating that the button is working. Must be 1 for UL installations.
***17**	**AC Loss Keypad Sounding** **0** = disable **1** = enable	If enabled, sounding at the keypad (rapid beeping) occurs when AC power is lost (sounding occurs about 2 minutes after actual AC loss).
***19**	**Randomize AC Loss Report** **0** = disable **1** = enable	If enabled, randomizes AC loss reporting between 10 and 40 min. after an actual AC loss. If disabled, AC loss reporting about 2 minutes after actual AC loss. Selecting this option helps prevent an overload of AC loss messages at the central station during a community blackout.
***20**	**VIP Module Phone Code** **1-9** = first digit of access code ***** or **#** = second digit of access code (enter 11 for "*", or 12 for "#") To disable enter **00** for the 1st digit	If a 4286 Voice Module is being used, enter the 2-digit phone code used to access the system. Must be disabled for UL installations.
***21**	**Prevent Fire Timeout** **0** = disable (timeout) **1** = enable (no timeout)	If enabled, there is no timeout of the alarm sounder duration for all fire zones, regardless of partition, so that fire sounding continues until the system is reset. If disabled, (timeout) the normal burglary sounder duration (field ✳13) applies to fire alarms.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***22**	**Keypad Panic Enables (partition-specific)** **0** = disable **1** = enable	If enabled, the keypad panics (zones 995, 996, and 999) may be used in this partition. There are three entries in this field, one for each panic.
***23**	**Multiple Alarms (partition-specific)** **0** = disable **1** = enable	If enabled, allows more than one alarm sounding for a given zone during an armed period. **NOTE:** that multiple alarm soundings will not occur more frequently than allowed by the programmed alarm sounder duration. This has no impact on the number of communication messages transmitted. Must be 1 for UL installations.
***24**	**Ignore Expansion Zone Tamper** **0** = disable (tamper detection) **1** = enable (no tamper detection)	If disabled, the system monitors the tampers on expansion zones. **NOTE:** Only applicable to certain polling loop sensors with tamper switches or 5800 Series transmitters. Must be **0** for UL installations.
***26**	**Intelligent Test Report** **0** = disable **1** = enable	If enabled, no test report is sent if any other type of report was sent since the last test report. If disabled, test reports are sent at the set intervals, regardless of whether or not any other report has been sent. Must be **0** for UL applications.
***27**	**Test Report Interval** Enter **0001-9999** for the test report interval in hours. Enter **0000** for test reporting.	If a test report is desired, enter a test code in *Report Code Programming* in *#93 Menu Mode*. Set first test report time in field *83. Maximum Test report interval is 0024 for UL installations.
***28**	**Power-Up in Previous State** **0** = disable **1** = enable	If enabled, the system, upon power-up, reverts to its status prior to a complete power loss. If disabled, the system always powers up in a disarmed state. **NOTE:** Neither authority level 0 nor 5 can be used to disarm the system if the control powers up armed. Must be **1** for UL applications.
***29**	**Quick Arm (partition-specific)** **0** = disable **1** = enable	If enabled, allows arming of the burglary system in AWAY, STAY, INSTANT, or MAXIMUM mode by using the [#] key instead of the user code. **NOTES:** When armed, the system reports closing as User 0 if Open/Close reporting for User #2 (typically a Master level user) was enabled for a given partition. If Quick Arm is used, the Installer Code and Authority Level 5 codes cannot disarm the system.
***30**	**Phone Linecut Detect** **0** = disable **1** = enable	Select phone linecut detection.
***31**	**PABX Access Code** Enter **00-09; B-F (11-15)**	This field is used to enter up to four 2-digit numbers representing the prefix needed to obtain an outside telco line. If not required, enter nothing and proceed to next field.
***32**	**Primary Subscriber's Account Number (partition-specific)** Enter **00-09; B-F (11-15)**	Enter a 4- or 10-digit (depending on report format) primary subscriber account number. Each number requires a 2-digit entry so as to allow entry of hexadecimal digits (B-F). If a 4-digit account number is to be used, enter data only in the first four locations, and enter * in the fifth location.
***33**	**Primary Phone Number** Enter **0-9; #11** for ***, #12** for **#, #13** for a 2-second pause.	Enter the primary central station phone number, up to 17 digits. This is the phone number the control will use to transmit Alarm and status messages to the central station. Do not fill unused spaces. **NOTE:** Backup reporting is automatic only if a secondary phone number is entered.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***34**	**Secondary Phone Number** Enter **0-9; #11** for *, **#12** for **#, #13** for a 2-second pause.	Enter the secondary phone number, up to 17 digits. The secondary phone number is used if communication on the primary number is unsuccessful, or if split/dual reporting is desired. Do not fill unused spaces. **NOTE:** If this field is programmed, a secondary subscriber account number (field *90) *must* also be programmed.
***35**	**Download Phone Number** Enter **0-9; #11** for *, **#12** for **#, #13** for a 2-second pause.	Enter the downloading phone number, up to 17 digits. Do not fill unused spaces. **NOTE:** This field is applicable only if downloading is utilized.
***36**	**Download ID Number** Make entries as 2-digit numbers as follows: 00=0 01=1 02=2 03=3 04=4 05=5 06=6 07=7 08=8 09=9 10=A 11=B 12=C 13=D 14=E 15=F	Enter eight digits. **NOTE:** This field is applicable only if downloading is utilized.
***37**	**Download Command Enables** **0** = disable **1** = enable	Enabling a function means that you are able to perform that function via the ADEMCO Compass Downloading software. Functions are as follows: Dialer Shutdown; System Shutdown; Not Used; Remote Bypass; Remote Disarm; Remote Arm; Upload Program; Download Program. For UL installations, all entries must be **0**.
***38**	**Prevent Zone XXX Bypass (partition-specific)** Enter a zone number **(001-250)**. Enter **000** if all zones can be bypassed.	Enter three digits for zone that cannot be bypassed by the user. **NOTES:** The actions manual bypass, group bypass, auto-stay, and STAY/INSTANT arming modes cannot bypass any zone programmed in this field. The system will not arm if the zone is programmed with the vent zone or force arm fault attributes. **ULC** Force Arming is not a ULC Listed feature and must be disabled for ULC installations.
***39**	**Enable Open/Close Report for Installer Code (partition-specific)** **0** = disable **1** = enable	If enabled, whenever the Installer Code is used to arm or disarm the partition, an open/close report is sent to the central station.
***40**	**Enable Open/Close report for Keyswitch** **0** = disable **1** = enable	If enabled, whenever the keyswitch is used to arm or disarm the partition, an open/close report is sent to the central station.
***41**	**Normally Closed or EOLR (Zones 2-8)** **0** = EOLR used **1** = normally closed	If 0, end-of-line resistors must be used on zones 2-8. If 1 end-of-line resistors cannot be used and only **normally closed** devices must be used. Must be **0** for UL installations.
***42**	**Dial Tone Pause** Enter the wait time for dial tone detection: **0** = 5 seconds; **1** = 11 seconds; **2** = 30 seconds.	Enter the time the system waits for dial tone before dialing. Must be **0** for UL installations.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***44**	**Ring Detection Count** Enter **00** to disable ring detection. Enter **01-14** for ring counts of 1-14. Enter **15** to select Answering Machine Defeat Mode	Only applicable if using a 4286 VIP Module and/or if station-initiated downloading will be used. **NOTES:** Do not enter 00 if a 4286 is installed. In the Answering Machine Mode, the caller should let the phone ring once, then hang up, and call again within 30 seconds. The system, upon hearing one ring followed by nothing, does not answer the first call, but readies itself to pick up on the first ring of the next incoming call that is received within 30 seconds (i.e., the downloader calling again). Must be **00** for UL installations.
***45**	**Primary Format** **1** = Contact ID; **2** = 10-Digit Contact ID; **3** = 4+2 Express	Enter the reporting format for the primary telephone number.
***47**	**Secondary Format** **1** = Contact ID; **2** = 10-Digit Contact ID; **3** = 4+2 Express	Enter the reporting format for the secondary telephone number.
***51**	**Dual Reporting** **0** = disable **1** = enable	If enabled, all reports are to be sent to both primary and secondary phone numbers. **NOTE:** If used with Split Reporting option 1 (1*34), alarms go to both primary and secondary numbers, while all other reports go to secondary only. If used with Split Reporting option 2, alarms go to both lines, open/close and test messages go to secondary only, while all other reports go to primary.
***56**	**Dynamic Signaling Delay** Enter **00-15** times 15 seconds.	Select the time the panel should wait for acknowledgment from the first reporting destination before it attempts to send a message to the second destination (first and second destinations are determined in field ✳57). **NOTE:** If the acknowledgment is received before the delay time expires, no message is sent to the second destination.
***57**	**Dynamic Signaling Priority** **0** = Primary Dialer **1** = Long Range Radio	Select the initial reporting path for central station messages.
***58**	**Long Range Radio Central Station #1 Category Enable** **0** = disable **1** = enable	This field has six entries as follows: Alarm, Trouble, Bypass, Open/Close, System and Test. If enabled, the reports are sent to the primary subscriber ID of the Communicator.
***59**	**Long Range Radio Central Station #2 Category Enable** **0** = disable **1** = enable	This field has six entries as follows: Alarm, Trouble, Bypass, Open/Close, System and Test. If enabled, the reports are sent to the secondary subscriber ID of the Communicator.
***79**	**Zone Type Restores for Zone Types 1-8** **0** = disable **1** = enable	This field has eight entries, one for each zone type. Select the zone types that will send Restore reports.
***80**	**Zone Type Restores for Zone Types 9, 10, 16 and 14** **0** = disable **1** = enable	This field has four entries, one for each zone type. Select the zone types that will send Restore reports.
***83**	**First Test Report Time** Enter **00-07** for the day (01 = Monday) Enter **00-23** for the hour Enter **00-59** for the minutes	Enter the day and time that the first Test report shall be transmitted. Enter **00** in all locations if the Test report is to be sent immediately upon exiting. Enter **00** in the day location if the report is to be sent at the next occurrence of the time that is set.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
***84**	**Swinger Suppression (partition-specific)** Enter **01-15**. Enter **00** for unlimited reports	This option limits the number of messages (alarms or troubles) sent for a specific zone in an armed period. Must be **00** for UL installations.
***85**	**Enable Dialer Reports for Panics & Duress (partition-specific)** **0** = disable **1** = enable	This field has four entries as follows: Zone 995, 996, 999, Duress Enable for each partition that the panics and duress reporting is desired. **NOTE:** Non-zero report code must be assigned to zone 992 (duress) to enable Duress reporting. If you enable any of the panics to report, make sure field *22 is programmed correctly for each partition.
***88**	**Burglary Alarm Communicator Delay (partition-specific)** **0** = no delay **1** = 30-second delay	Select the delay, if any, for burglary alarm communications. Must be **0** for UL installations.
***89**	**Restore Report Timing** **0** = instant **1** = after bell timeout **2** = when system is disarmed	Select the time when restore reports are sent after an alarm. Must be **2** for UL installations.
***90**	**Secondary Subscriber Account Number (partition-specific)** Enter **00-09; B-F (11-15)**	Enter a 4- or 10-digit (depending on report format) primary subscriber account number. Each number requires a 2-digit entry so as to allow entry of hexadecimal digits (B-F). If a 4-digit account number is to be used, enter data only in the first four locations, and enter * in the fifth location. **NOTE:** This field *must* be programmed if a secondary phone number is used (field *34). This account number can be the same as the primary account number.
1*07	**Check or TRBL Display** **0** = CHECK **1** = TRBL	Select whether the system should display TRBL or CHECK for trouble conditions.
1*11	**Zone Bypass After Disarm** **0** = disable **1** = enable	This field has eight entries, one for each partition. For each partition in which "1" is entered, zones will remain bypassed after the system is disarmed.. **NOTES:** For each partition in which field 1✳11 is enabled, the **USER CODE + OFF** will no longer unbypass zones. To unbypass ALL zones, you must enter **USER CODE + # + 64.** To unbypass zones INDIVIDUALLY, you must enter **USER CODE + 6 + zone number**. Any zone that was automatically bypassed by the system will be unbypassed upon disarming of the system (e.g., STAY mode, Auto-STAY, etc.). Vent zones and zones bypassed by a programmed Auto-Bypass schedule (Timed Driven Event) are considered "manual bypasses" and will not be unbypassed upon disarming the system. Zones that were in a bypassed state at the time a System Shutdown is sent from the Compass Downloading software will be unbypassed when the System Shutdown is removed.
1*15	**Cancel Verify** **0** = disable **1** = enable alarm output pulse upon kissoff of Cancel report.	**NOTE:** Field 1✳52 must be enabled to send a Cancel report to the central station.
1*17	**Lobby Partition** **0** = none **1-8** = partition number	Select the Common Lobby Partition.
1*18	**Affects Lobby (partition-specific)** **0** = disable **1** = enable	If enabled, causes lobby partition to disarm when this partition disarms. **NOTE:** This partition must be armed before lobby can be armed.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*19	**Arms Lobby (partition-specific)** **0** = disable **1** = enable	If enabled, arming this partition causes the system to attempt to arm the lobby partition automatically. To enable this field, field 1*18 must also be enabled (partition-specific). **NOTES:** The lobby cannot be armed unless all partitions programmed for "affect" (field 1*18) is already armed. If his field is enabled, Field 1*18 for this partition must also be enabled.
1*20	**Exit Error Logic Enable** **0** = disable **1** = enable	Exit Error Logic functions as follows: the system at the end of the exit delay, if a door is left open or an interior zone is faulted, starts the entry delay period, and sounds the bell(s), siren(s), and keypad sounders for the duration of entry delay. This gives the user time to re-enter the premises and disarm the system before exit error occurs. If the user does not re-enter the premises and disarm the system, the system bypasses the faulted entry/exit and/or interior zone(s). The rest of the system is armed. In addition, the following dialer reports are sent to the central station if programmed: Exit Error by Zone Entry/Exit or Interior Alarm with the zone number Bypass reports

UL Exit Error Logic is not suitable for use in a UL installation.

1*21	**Exit Delay Reset** **0** = disable **1** = enable	If enabled, when the panel is armed, the normal exit delay begins. After the user exits, closes the door and then re-enters the premises, the exit delay time is reset to the programmed value. **NOTES:** Exit Delay Reset is designed to allow an operator to re-enter the premises to retrieve a forgotten item without triggering an alarm. This feature may only be activated once after arming.

UL Exit Delay Reset is not suitable for use in a UL installation.

Cross-Zoning

UL Cross Zoning is not suitable for use in a UL installation.

Cross Zoning is designed so that a combination of two zones must be faulted within a 5-minute period of each other (whereas the first zone remains faulted, when the second zone trips) to cause an alarm on either zone. This prevents momentary faults from one of the zones from causing an alarm condition.

You can select four "sets" of cross-zones (programmed in data fields 1*22, 1*23, 1*24, and 1*25), keeping in mind the following:

- Both zones in each set must protect the same area.
- When cross-zoning motion sensors, both device's areas of protection must be situated so that both units will trip at the same time if their shared protected area is violated.
- Both zones in each set must be in the same partition.

DO NOT cross-zone a fire zone with a burglary zone under any circumstance. DO NOT cross a fire zone with another fire zone under any circumstance.

Conditions That Affect Cross-Zone Operation

- If one of the zones in a pair is bypassed or has a zone response type set to 0, the cross-zoning feature does not apply.
- If an entry/exit zone is paired with an interior follower zone, be sure to enter the entry/exit zone as the first zone of the pair. This ensures that the entry delay time is started before the follower zone is processed.
- If a relay is programmed to activate on a fault of one of the zones, the relay activates without the other zone being faulted.
- If a relay is programmed to activate on either an alarm or trouble, both zones must trip before the relay will activate, and both zones must restore for the relay to deactivate (if relay is programmed to deactivate on a Zone List Restore).

If the one of the zones trips and the second zone does not trip within the 5-minute period, an "error" message is reported to the central station. The Contact ID event code is 378.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*22	**Cross Zoning Pair One** Enter **001-250** Enter **000,000** to disable	Select the first pair of cross zones, which must both be faulted within a 5-minute period to cause an alarm. Must be 000,000 for UL installations.
1*23	**Cross Zoning Pair Two** Enter **001-250** Enter **000,000** to disable	Select the second pair of cross zones, which must both be faulted within a 5-minute period to cause an alarm. Must be 000,000 for UL installations.
1*24	**Cross Zoning Pair Three** Enter **001-250** Enter **000,000** to disable	Select the third pair of cross zones, which must both be faulted within a 5-minute period to cause an alarm. Must be 000,000 for UL installations.
1*25	**Cross Zoning Pair Four** Enter **001-250** Enter **000,000** to disable	Select the fourth pair of cross zones, which must both be faulted within a 5-minute period to cause an alarm. Must be 000,000 for UL installations.
1*26	**Panic Button or Speedkey** For A, B, C keys: **00** = panic function **01-32** = macro number For D key: **00** = to select a macro to execute when key is pressed **01-32** = macro number	Select for the A, B, and C keys whether the system performs a panic or a speedkey function when the key is pressed. Select for the D key whether the system performs a specific macro or if the user will select a macro when the key is pressed. **NOTES:** If using the A, B, and C, keys for panic alarms, verify fields *22 and *85 are programmed correctly. If a user code with global arm/disarm is used to execute the macro, the user's global capabilities will override any arm/disarm commands in the macro sequence.
1*28	**RF Transmitter Low Battery Sound** **0** = disarmed state only **1** = both armed and disarmed states	Select when the RF transmitter low-battery condition should display and audible beep annunciate on the keypad. Must be **1** for UL installations.
1*29	**RF Transmitter Low Battery Reporting** **0** = disable **1** = enable	If enabled, the system sends a Trouble message for RF transmitter low-battery condition to the central station. **NOTE:** The Trouble message will be sent for a transmitter supervision failure, independent of this selection. Must be **1** for UL.
1*30	**RF Receiver Supervision Check-in Interval** Enter **02-15** times 2 hours (4-30 hours). **00** = disable receiver supervision.	Select the check-in monitoring interval for the RF receiver(s). Failure of a receiver to receive any RF signal within the time entered results in the activation of the response type programmed for zone 990 for the first receiver and zone 988 for the second receiver and their related communication reports. Maximum is 2 (4 hr) for UL installations.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*31	**RF Transmitter Check-in Interval** Enter **02-15** times 2 hours (4-30 hours). **00** = disable transmitter supervision.	Select the check-in monitoring interval for the RF transmitters. Failure of an individual transmitter to send a supervision signal within the time entered will result in a trouble response and related communication report. Maximum is 2 (4 hr) for UL.
1*34	**Communicator Split Reporting** **0** = Split Reporting disabled **1** = Alarm, Alarm Restore, and Cancel reports to primary, all others to secondary **2** = Open/Close and Test reports to secondary, all other reports to primary	Select the type of split reporting for system communication. **NOTE:** See *51 for split/dual reporting combinations. **NOTE:** Split reporting should not be used with Dynamic Signaling.
1*35	**Access Control Dialer Enables** **0** = disable **1** = enable	There are six entries for this field as follows: Trace, Trouble, Not Used, Bypass, System and Alarm. If Trace is enabled, access grant/denial events sent to the central station. For the other events, if enabled, a report is sent to the central station. **NOTE:** When Access Control and/or Home Automation is in use, Opening Reports and Trace Reports are delayed 60 seconds.
1*42	**Call Waiting Defeat** **0** = disable **1** = enable	If enabled, the system defeats Call Waiting on the first outgoing call attempt to both the primary and secondary numbers. **NOTES:** After the panel's initial call to report the alarm, the panel may attempt to make an additional call, perhaps for a cancel or a zone restoral. If Call Waiting is not defeated, an operator at the central station attempting to contact the premises (to verify whether the alarm is valid) hears the phone ringing indefinitely and must to dispatch on the call. **DO NOT enable this feature unless Call Waiting is being used.**
1*43	**Permanent Keypad Display Backlighting (partition-specific)** **0** = disable **1** = enable	If enabled, backlighting for the keypad display remains on at all times. Otherwise the backlighting comes on when a key is pressed. **NOTE:** When a key is pressed, display backlighting turns on for **all** keypads in that partition. **NOTE:** This field affects only standard keypads, not graphic/touch-screen keypads.
1*44	**Wireless Keypad Tamper Detect** **0** = disable **1** = enable	If enabled, when more than 40 key depressions are received without a valid sequence (arm, disarm, etc.), the control panel disables the wireless keypad. The inhibit is removed once a valid key sequence is received from a wired keypad. **UL** Wireless Keypad is not suitable for use in a UL installation.
1*45	**Exit Delay Sounding (partition-specific)** **0** = disable **1** = enable	If enabled, the system produces slow beeping from the keypads during exit delay and reverts to rapid beeping during the last 10 seconds of the exit delay. **NOTES:** Must be set to "1" for UL/ULC installations. The duration of the beeping is the programmed value of field *10 regardless of which entry/exit zone is used to exit the premises. See page 30 in the *Programming Guide*, "SOUND OPTION", prompt for disabling the entry/exit beeps on individual keypads.
1*46	**Auxiliary Output Mode** **0 =** Not used **1** = smoke detector reset. **2** = Not used **3** = AAV module.	Select the mode for output 1 on the J7 triggers. **NOTES:** Only one of the options may be active within the system.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*47	**Chime On Ext. Siren (partition-specific)** **0** = disable **1** = enable	If enabled, the system produces chime annunciation on the external alarm sounder.
1*48	**Wireless Keypad Assignment** **0** = none **1-8** = partition number	Select the partition in which RF keypad is used. **UL** Wireless Keypad is not suitable for use in a UL installation.
1*49	**Suppress Transmitter Supervision Sound** **0** = disable **1** = enable	If enabled, no trouble soundings occur on the keypad for transmitter check-in failures. Must be **0** for UL.
1*52	**Send Cancel If Alarm + Off (partition-specific)** **0** = disable **1** = enable	If enabled, Cancel reports are sent when the system is disarmed after an alarm, regardless of how much time has gone by. If disabled, Cancel reports are sent within Bell Timeout period only. **NOTES:** This option must be enabled so Cancel reports are always sent.
1*53	**Disable Download Callback** **0** = callback required **1** = no callback required	Select whether a callback from the control panel is required for downloading. Must be **0** for UL installations.
1*55	**International Date Format** **0** = disable (mm/dd/yy) **1 =** enable (dd/mm/yy)	Select the date format for display in the event log.
1*56	**AC 60Hz/50Hz** **0** = 60Hz **1** = 50Hz	Select the frequency for the AC. Must be set to **0** for U.S. and Canadian installations.
1*57	**Enable 5800 RF Button Global Arm** **0** = disable **1** = enable	If enabled, the system arms/disarms in accordance with the button's user's global arming settings.
1*58	**Enable 5800 RF Button Force Arm** **0** = disable **1** = enable	If enabled, allows the RF button user to force a bypass of all faulted zones when arming the system. **NOTE:** When attempting to arm the system, the keypad beeps once after the button is pressed if any faulted zones are present. **ULC** Force Arming is not a ULC Listed feature and must be disabled for ULC installations.
1*60	**Zone 5 Audio Alarm Verification** **0** = disable **1** = enable	If enabled, zone 5 is used for 2-way audio (AAV). Must be 0 for UL installations. **NOTE:** Zone 5 cannot be used as protection zone.
1*70	**Event Log Types** **0** = disable **1** = enable	This field has five entries as follows: Alarm, Check, Bypass, Open/Close and System. If enabled, the system logs those events into the event log.
1*71	**12/24 Hour Type Stamp Format** **0** = 12-hour **1** = 24-hour	Select the type of time stamping for the event log.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*72	**Event Log Printer On-Line Mode** **0** = disable **1** = enable	If enabled, the system prints the events as they occur. If disabled, the system prints the log only upon request.
1*74	**Relay Timeout XXX Minutes** Enter **000-127** times 2 minutes (000-254).	This is used for #80 Menu Mode Time-Driven event relay command numbers "04/09" and *Output Programming* in the *#93 Menu Mode Programming* output command "56."
1*75	**Relay Timeout YYY Seconds** Enter **000-127** seconds.	This is used for #80 Menu Mode Time-Driven event relay command numbers "05/10" and *Output Programming* in the *#93 Menu Mode Programming* command "57."
1*76	**Access Control Relay (partition-specific)** **01-96** = relay number **00** = relay not used.	If enabled, the assigned relay closes for 2 seconds when the user enters his code and presses 0. Must be **00** for UL installations.
1*77	**Log 1st Main Signal** **0** = disable **1** = enable	If enabled, the system logs the first maintenance signal from each smoke detector. If disabled, no logging occurs.
1*78	**Extended Home Control Enable** **0** = limited **1** = extended	If extended, there are 255 commands to the home control command set. If limited, there are 32 commands to the home control command set. Home Control Automation is not allowed in UL installations.
1*79	**Home Control Events** **0** = disable **1** = enable	This field has five entries as follows: Alarm, Trouble, Bypass, Open/Close, and System. Select the type of events (status reports) transmitted via the RS232 output (TB4). Home Control Automation is not allowed in UL installations.
1*80	**Log Faults & Restores** **0** = disable **1** = enable	When enabled automatically transfers zone fault/restore data of the RS232 output (TB4). Home Control Automation is not allowed in UL installations.
2*00	**Number of Partitions** Enter **1-8**.	Enter the number of partitions used in the system.
2*01	**Daylight Saving Time Start/End Month** **0** = disable **1** = enable	Enter the months (**00-12)** in which daylight saving time starts and ends. Enter **00, 00** if daylight saving time does not apply to the user's region. Standard setting for U.S. is 03,11.
2*02	**Daylight Saving Time Start/End Weekend** **0** = disable **1** = enable	Enter the start and end weekends for daylight saving time as follows: 1=first; 2=second; 3=third; 4=fourth; 5=last; 6=next to last; 7=third from last. Standard setting for U.S. is 2,1.
	UL Fields 2*05 – 2*08 must be set to 0 for UL installations.	
2*05	**Auto-Arm Delay (partition-specific)** **00** = no delay. **01-14** times 4 minutes (04-56) delay. **15** = no auto arming.	This is the time between the end of the arming window and the start of auto-arm warning time (field 2*06).

FIELD	TITLE and DATA ENTRIES	EXPLANATION
2*06	**Auto-Arm Warning Period (partition-specific)** **01-15** times 1-minute warning. **00** = no warning period.	This is the time that the user is warned by a keypad sounding and display to exit the premises prior to auto arming of the system.
2*07	**Auto-Disarm Delay (partition-specific)** **00** = no delay. **01-14** times 4 minutes (04-56) delay. **15** = no auto disarming.	This is the time between the end of the disarming window and the start of auto disarming of the system.
2*08	**Force Arm Enable for Auto-Arm (partition-specific)** **0** = disable **1** = enable	If enabled, the system automatically bypasses any faulted zones when it attempts to auto-arm. If disabled, the system will not auto-arm. **ULC** Force Arming is not a ULC Listed feature and must be disabled for ULC installations.
2*09	**Open/Close Reports by Exception (partition-specific)** **0** = disable **1** = enable	If enabled, Open/Close reports are sent **only if** the openings/closings occur **outside** the arm and disarm windows. **NOTES:** Open reports are also suppressed during the closing window in order to prevent false alarms if the user arms the system, then re-enters the premises, for example to retrieve a forgotten item. Openings and closings are still recorded in the event log.
2*10	**Allow Disarming Only During Arm/Disarm Windows (partition-specific)** **0** = disable **1** = enable	If enabled, disarming of the system is allowed only during the arming/disarming windows, or if the system is in alarm (if 2*11 is set to 1). **NOTE:** This applies **only** to Operator-level users. Installer, Master, and Manager-level users can disarm the system at any time. **NOTE:** Duress users behave the same way as Operator-level users.
2*11	**Allow Disarm Outside Window if Alarm Occurs** **0** = disable **1** = enable	If enabled, allows the system to be disarmed outside the programmed disarm (opening) window if an alarm has occurred. Otherwise disarming is allowed only during the disarm window. **NOTE:** Used only if field 2*10 is enabled.
2*18	**Enable GOTO for this Partition (partition-specific)** **0** = disable **1** = enable	If enabled, this partition can be accessed from another partition's keypad using the GOTO command.
2*19	**Use Partition Descriptor** **0** = disable **1** = enable	If enabled, the normal keypad display will include a partition number and four-digit descriptor.
2*22	**Display Fire Alarms of Other Partitions (partition-specific)** **0** = disable **1** = enable	If enabled, allows fire alarms that occur on other partitions to be displayed at this partition's keypad(s).
2*23	**Display Burg, Panic and CO Alarms for Other Partitions (partition-specific)** **0** = disable **1** = enable	If enabled, allows burglary, panic and CO alarms that occur on other partitions to be displayed at this partition's keypad(s).
2*24	**Display Troubles of Other Partitions (partition-specific)** **0** = disable **1** = enable	If enabled, allows troubles that occur on other partitions to be displayed at this partition's keypad(s).

Scheduling Options

UL

- You must program Bypass and Auto-Arm Fail reports for UL installations.
- Auto-disarming is not permitted in UL installations.
- You must not program Random Scheduling of Time Driven Events for UL installations.

ULC Scheduling is not approved for use in ULC installations.

General

The scheduling features allow certain operations to be automated, such as arming, disarming, bypassing of zones, and activating relay outputs.

The system uses time windows (a programmed period of time with a start and stop time) for defining open/close schedules, holiday schedules, user-defined temporary schedules, and access schedules for users.

Scheduled events are programmed by user-friendly menu modes of programming (#80, #81, #83, and #93 modes), explained in detail in this section. These menus take you step by step through the options.

Auto Arming

ULC Auto Arming is not a ULC Listed feature.

The system can automatically arm (AWAY Mode) a partition at the end of a pre-determined closing (arming) time window.

Auto Arming can be delayed three ways: by use of the Auto-Arm Delay, the Auto-Arm Warning, or by manually extending the closing (arming) time window with a keypad command.

The system can also automatically bypass any open zones when auto arming.

Auto-Arm Delay

Auto-Arm Delay provides a delay (grace period) before auto arming. It starts at the end of the closing time window.

The delay is set in 4-minute increments, up to 56 minutes in partition-specific program field 2*05. At the expiration of this delay, the Auto-Arm Warning will start.

Auto-Arm Warning

The Auto-Arm Warning causes the keypad sounder to warn the user of an impending Auto-Arm.

The warning can be set from 1 to 15 minutes prior to the arming in partition-specific program field 2*06. During this period the keypad beeps every 15 seconds and displays “AUTO ARM ALERT.” During the last 60 seconds, the keypads beep every 5 seconds.

The panel arms at the conclusion of the Auto-Arm Warning period.

Extend Closing Window

A user can manually delay the arm (closing) time window by 1 or 2 hours. This is done by entering a keypad command (User Code + **#82**), which then prompts the user to enter the desired extension time of 1 or 2.

This feature is useful if a user must stay on the premises later than usual.

The Auto-Arm delay and warning periods begin at the end of the extension.

Force Arm

ULC Force Arming is not a ULC Listed feature and must be disabled for ULC installations.

The Force Arm option causes the panel to attempt to bypass any faulted zones prior to auto arming (panel performs a force-arm).

This option is set in partition-specific program field 2*08.

Auto Disarming

The system can automatically disarm a partition at the end of a pre-determined opening (disarm) time window.

The disarming time can be delayed by using the Auto-Disarm Delay feature.

Disarm Delay

Auto-Disarm Delay provides a delay before auto disarming. This delay is added to the end of the disarm time window.

The delay is set in 4-minute increments, up to 56 minutes, in partition-specific program field 2*07.

Restrict Disarming

This option allows disarming by users only during the disarm time window and during the arming time window (in case user needs to re-enter premises after manually arming the partition).

This option is set in partition-specific field 2*10. If field 2*10 is set, we highly recommend setting field 2*11, as well. This field allows the partition to be disarmed outside the arm/disarm time windows only if the partition is in alarm.

Exception Reports

This option allows the reporting of openings and closings to the central station only if the arming and disarming occurs outside of the predetermined opening and closing time windows. It is set in partition-specific field 2*09.

The system can be programmed to send Failed to Open and Failed to Close reports if the partition is not armed or disarmed by the end of the corresponding time window.

Limitation of Access of Users by Time

A user's access to the system can be limited to a certain time period. Outside this time, that user's code is inactive. The system provides up to eight access schedules, each consisting of two time windows (typically one for opening, one for closing) for each day of the week and two time windows for holidays.

The access schedules are programmed in the #80 Menu Mode, and enabled when a user's access code is added to the system.

If a user tries to operate the system outside the schedule, the alpha keypad displays "Access Denied."

Time-Driven Events

The system can automatically activate and de-activate relays at predetermined times to turn lights or other devices on and off. The Time-Driven events can be activated at different times in relation to a time window:

- At the beginning of a time window
- At the end of a time window
- During a time window (on at beginning of window, off at end)
- At both the beginning and end of the time window (e.g., to sound a buzzer at the beginning and end of a coffee break)
- Random time at the start of the time window (occurs within 30 minutes after the start of the time window)
- Random time at the end of the time window (occurs within 30 minutes after the end of the time window)
- Random during the time window (begins within 30 minutes after the start of the time window and ends within 30 minutes after the end of the time window)

The system can perform the same actions on a daily basis, or can perform an action only once (e.g., turn on the porch light this Wednesday at 8:00 PM).

The system also provides up to 20 programmable "timers" available to the end user for the purpose of activating output devices at preset times and days.

Time Window Definitions

Scheduled events are based on time windows, (periods of time) during which an event may take place. The system supports up to 20 time windows, each defined by a "Start" time and a "Stop" time.

The windows are shared by all eight partitions, and are used when programming the various schedules (open/close, limitation of access), as well as for Time-Driven event control.

Scheduling Example

A store that has the following hours:

Monday to Friday	**9am to 6pm**
Saturday	**10am to 4pm**
Sunday	**Closed**
Holidays	**Closed**

The owner desires the following time windows to allow time for employees to arm or disarm the system:

Monday to Friday	**Open (disarm)**	**8am to 9am**
	Close (arm)	**6pm to 6:30pm**
Saturday	**Open (disarm)**	**9am to 10am**
	Close (arm)	**4pm to 4:30pm**
Sunday & Holidays	**Closed**	

For this schedule, the four time windows need to be programmed:

Window	Start	Stop	Purpose
1	8am	9am	Monday-Friday open window
2	9am	10am	Saturday open window
3	4pm	4:30pm	Saturday close window
4	6pm	6:30pm	Monday-Fri. close window

Using the #*80 Menu Mode*, the installer can program open/close schedules by assigning a time window to a day of the week (windows are entered as 2-digit entries)

Mon	Tue	Wed	Thu	Fri	Sat	Sun	Hol
Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl	Op/Cl
01/04	01/04	01/04	01/04	01/05	02/03	00/00	00/00

NOTE: 00 is entered for those days on which the store is closed.

Employees can arm and disarm the system, when programmed, within the open and close time windows without causing a report to be sent to the central station (reporting by exception, field 2*09). The system can be programmed to automatically arm/disarm in case an employee fails to arm/disarm manually (auto-arm/auto-disarm).

Open/Close Schedules Definitions

General

The open/close scheduling is controlled by one of three schedules. Each schedule consists of one time window for openings and one time window for closings.

There are three types of schedules available: Daily, Holiday, and Temporary.

Daily Schedule

Each partition can have one daily schedule consisting of one opening window and one closing window per day.

Holiday Schedule

A holiday schedule overrides the regular daily schedule on selected holidays throughout the year.

The opening and closing windows are programmed in the daily schedule, but the holidays themselves are defined in *Holiday Schedule Programming* in the #*80 Menu Mode*.

Temporary Schedule

The temporary schedule provides a method for the end user to override the daily and holiday schedules. It consists of one opening window and one closing window for each day of the week. The schedule takes effect for up to one week, after which it is automatically deactivated.

This schedule is programmed using the #81 Temporary Schedule Menu Mode.

Additional Schedules

Additional opening and closing schedules can be programmed using the *Time-Driven Event Programming*. For example, a schedule for normal store openings/closings can be programmed with a daily open/close schedule, and another open/close schedule for a lunch hour can be programmed using the Time-Driven event schedule programming.

Refer to "Time-Driven Events" later in this section for detailed information.

Open/Close Reports by Exception

The system can help reduce communication traffic to the central station by using the Open/Close Reports by Exception feature. The Open/Close by Exception option suppresses these reports from being sent to the central station if an arm or disarm is done ***within*** the expected time window. Reports are only sent if the arm or disarm occurs outside the assigned time window.

The system keeps a record of ***all*** openings/closings in its event log.

If a disarming occurs during a closing window (for example, a person who arms the system forgets something and has to re-enter), the Opening report (although outside of the opening window) will not be sent (as long as that disarming occurs within the closing window).

This option is programmed in partition-specific program field 2*09.

Example of Open/Close Exception Reporting & Scheduling

The following chart gives an example of how the Open/Close by Exception reporting works.

6:01PM 5:59AM	6AM 9AM	9:01AM 3:59PM	4PM 6PM	6:01PM 5:59AM
Early Opening reports are sent if system is manually disarmed before opening window begins. **Early and Late Opening and Closing reports are programmable options in the Report Code Programming. They are not dependent on the programming of the Exception Reporting option.**	Opening Window No reports are sent if system is disarmed during this time window. **If an arming occurs, a Closing report is sent to the central station regardless of how the Exception Reporting option is set.**	Auto-disarm delay begins. Auto-disarm occurs after delay (if auto-disarm is enabled). Missed Opening reports are sent if manual disarming has not occurred at expiration of opening window. Late Opening reports are sent if disarm occurs after the opening window expires. Early Closing reports are sent if manual arming occurs before the closing window begins. **Missed Opening/Closing type reports are programmed in the Report Code Programming. The Exception Reporting option must be set for these to be sent.**	Closing Window No reports are sent if system is armed* during this time window. * or disarmed if user needs to re-enter premises.	Auto-arm delay begins. Auto-arm warning begins. Auto-arm occurs after warning expires (if auto-arm is enabled). Missed Closing reports are sent if manual arming has not occurred at expiration of closing window. Late Closing reports are sent if system is manually armed after the closing window expires.

Scheduling Menu Mode

The #80 Scheduling Menu Mode is used to program most of the scheduling and timed-event options. Enter **Installer Code + [#] + [8] + [0]** from the normal operating mode. **NOTE:** Only users with an Installer or Master level user code may enter the #80 mode.

The following can be programmed while in this mode:

- time windows
- open/close schedules to each partition
- holiday schedules
- Time-Driven events (for system functions and relay activation)
- limitation of access schedules

Some scheduling features are programmed in Data Field Programming Mode (**Installer Code + 8 0 0 0**). Some features are programmed in the #93 Menu Mode. The programming scheduling fields are listed below.

System-Wide Fields:	
*04	Enable Random Timers
1*74 –1*75	Relay timeout values
2*01-2*02	Daylight saving time options
2*11	Allow disarming outside window if alarm occurs
Partition-Specific fields:	
2*05	Auto-arm delay value
2*06	Auto-arm warning time
2*07	Auto-disarm delay value
2*08	Force-arm enable
2*09	Open/Close Reporting by Exception
2*10	Restrict disarm only during windows
#93 Menu Mode (System Group #3)	
Scheduling related report codes	

Event-driven options are programmed using *Output Programming* in #93 *Menu Mode*. Relay activation can also be Time-Driven and that those are programmed using the *#80 Menu Mode*. Refer to the *Time-Driven Event Programming* later in this section for the procedure.

Steps to Program Scheduling Options

This section contains examples of the worksheets only. For complete worksheets, see the Programming Guide accompanying this Installation and Setup Guide.

In order to use #80 Scheduling Menu Mode, use the worksheets to do the following:

1. Define time windows (up to 20)
2. Define the daily open/close schedules (one schedule per day, per partition)
3. Define the holidays to be used by the system (up to 16)
4. Define limitation of access times (up to 8 schedules)
5. Define the Time-Driven events (up to 20)

NOTE: Temporary schedules are programmed using #81 Menu Mode.

Use #80 Scheduling Menu Mode to perform the following functions:

6. Program the time windows
7. Program the open/close schedules
8. Program the Time-Driven events
9. Program the access schedules

Scheduling Menu Structure

To program schedules, enter Scheduling Program Mode:

Installer Code + [#] + [80]. (Installer or Master level user code.)

Scheduling Program Mode can be entered only when all partitions are disarmed.

There are 6 sections of scheduling menus accessed via #80, as shown below. Entering **1** at a displayed main menu prompt selects that menu section. Prompts for programming that scheduling feature then appear. Enter **0** to skip a section and display the next menu option.

PROMPT	EXPLANATION
Time Window ? 1 = YES 0 = NO 0	Upon entering Schedule Menu Mode, this prompt appears. Enter **1** to program time windows. Refer to *Time Windows Programming* later in this section for detailed procedures. Enter **0** to move to the "O/C Schedules?" prompt.
O/C Schedules ? 1 = YES 0 = NO 0	Enter **1** to program opening and closing schedules. Refer to *Open/Close Schedules Programming* later in this section for detailed procedures. Enter **0** to move to the "Holidays?" prompt.
Holidays ? 1 = YES 0 = NO 0	Enter **1** to program holiday schedules. Refer to *Holiday Schedule Programming* later in this section for detailed procedures. Enter **0** to move to the "Timed Events?" prompt.
Timed Events ? 1 = YES 0 = NO 0	Enter **1** to program timed events for relay outputs, additional schedules, and other system functions. Refer to *Time-Driven Event Programming* later in this section for detailed procedures. Enter **0** to move to the "Access Sched?" prompt.
Access Sched. ? 1 = YES 0 = NO 0	Enter **1** to program access schedules. Refer to *Limitation of Access Schedules Programming* later in this section for detailed procedures. Enter **0** to move to the "Quit?" prompt.
Quit ? 1 = YES 0 = NO 0	Enter **1** to quit *#80 Scheduling Menu Mode* and return to normal operating mode. Enter **0** to make any changes or review the scheduling programming options. If you press **0**, the "Time Window?" prompt is displayed.

Time Windows

The system provides 20 time windows that are defined with start and stop times. These windows are used for various open/close and access schedules, as well as for output controls, and are the basis of the scheduling system. These windows are shared among all eight partitions.

Time Windows Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. This worksheet will help you define time windows and scheduling aspects of this system before you program them. Note that time windows **can** span midnight; for example, from 11 PM to 1 AM.

Time Window Number	Start Time (HH:MM)	Stop Time (HH:MM)
1		
2		
3…..20		

A time window must have a start and a stop time.

Time Windows Programming

Enter Scheduling Mode by entering **Installer Code + [#] + [80]**. The keypad displays the *Time Window Programming* prompt.

PROMPT	EXPLANATION
Time Window ? 1 = YES 0 = NO 0	Enter **1** at this main menu prompt to program time windows.
Time Window # ? 01-20, 00 = Quit 01	Enter the 2-digit time window number **(01-20)** to be programmed. Press [✳] to accept the entry. Enter **00 + [✳]** at the "Time Window #?" prompt to quit time window programming and display the "Quit ?" prompt.
01 TIME WINDOW 00:00AM 00:00AM	If you entered a time window number, the cursor is now positioned on the tens of hours digit of the start of window entry. Enter the desired start of window hour and press [✳]. The cursor moves to the minutes position. Enter the desired minutes and press [✳]. Toggle the AM/PM indication by pressing any key 0-9 while the cursor is under the A/P position and then press [✳]. Repeat this to program the stop of window entry. When the entry is completed, the "Time Window #?" prompt is displayed again. Enter the next time window number to be programmed and repeat the procedure.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the Quit ? prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Because the time windows are shared among all partitions, it is important to make sure that changing a time window does not adversely affect desired actions in other partitions.

Daily Open/Close Schedules

Each partition can be assigned one daily open/close schedule, plus a holiday schedule. Temporary schedules are programmed separately, using the *#81 Temporary Schedule Menu Mode*. To program additional open/close schedules, see *Time-Driven Events Programming* later in this section for the procedure.

Open/Close Schedule Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. Write the previously defined time window numbers for open and close for each partition.

Part	Mon		Tues		Wed		Thur		Fri		Sat		Sun		Hol	
	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl
1																
2																
3…8																

Open/Close Schedule Programming

After entering Scheduling Menu Mode, press **[0]** until the "O/C Schedules?" prompt appears.

PROMPT	EXPLANATION
O/C Schedules ? 1 = YES 0 = NO 0	Enter **1** to program opening and closing schedules.
Partition # ? 01-08, 00 = Quit 01	Enter the appropriate partition number for which the following open/close schedules will apply. Enter **00 + [✳]** at the "Partition #?" prompt to quit open/close schedules programming and display the "Quit ?" prompt.
Mon P1 OP WIND.? 00:00 00:00 00	Enter the time window number **01-20** for the displayed day's opening schedule beginning with Monday. Enter **00** if no schedule is desired for a particular day. As the number is keyed in, the actual time that has been stored for that window number is displayed as a programming aid. Press [✳] to accept the entry.
Mon P1 CL WIND.? 00:00 00:00 00	Enter the time window number for the displayed day's closing schedule. As the number is keyed in, the actual time that has been stored for the window number is displayed. Press the [✳] key to accept the entry.
Tue P1 OP WIND.? 00:00 00:00 00	The keypad now prompts for Tuesday's open/close schedule. Follow the procedure for Monday's prompts. When the last day of the week has been programmed, the holiday opening and closing window prompts are displayed.
Hol P1 OP WIND.? 00:00 00:00 00	Repeat the procedure for the holiday opening and closing time windows. Press the [✳] key to accept the entry. When the entries are completed, the "Partition #?" prompt is displayed again. Repeat this procedure for each partition in the system.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Holiday Schedules

A holiday schedule overrides the regular daily open/close schedule on the programmed holidays throughout the year.

The system provides up to 16 holidays that can be assigned for the system. Each holiday can be assigned to any combination of partitions. List the desired holidays in a Month/Day format on the worksheet. Check the partitions for which these holidays apply.

Holiday Schedule Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*.

HOL	Partition								
	Month/Day	1	2	3	4	5	6	7	8
1	/								
2	/								
3…16									

Holiday Schedule Programming

After entering Scheduling Menu Mode, press **[0]** until the "Holidays ?" prompt appears.

PROMPT	EXPLANATION
Holidays ? 1 = YES 0 = NO 0	Enter **1** to program holiday schedules.
HOLIDAY NUMBER ? 01-16,00=Quit 01	Enter the 2-digit holiday number **(01-16)** to be programmed and press [✳] to accept entry. Enter **00 + [✳]** at the "Holiday Number?" prompt to quit the holiday menus and display the "Quit ?" prompt.
01 ENTER DATE 00/00	The cursor is now positioned on the tens of months digit. Enter the appropriate month, then press [✳] to proceed to the day field. Enter the appropriate day for the holiday. Press [✳] to accept the entry.
Part ? 12345678 Hit 0-8 x x	Holidays can be set for any partition, as follows. Press **[0]** to turn all partitions on or off, or use keys **1-8** to toggle the letter "x" under the partition to which this holiday will apply. Press the [✳] key when all desired partitions have been assigned. The "Holiday Number?" prompt is displayed again. Repeat the procedure for each holiday to be programmed.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Time-Driven Events

These schedules are used to activate outputs, bypass zones, etc. based on time. There are 20 of these schedules that may be programmed for the system, each governed by the previously defined time windows.

The actions that can be programmed to automatically activate at set times are: relay commands, arm/disarm commands, zone bypassing commands, and open/close access conditions.

Time-Driven Events Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. Fill out the worksheet using the steps outlined below.

Sched Num.	Time Window	Days								Action Desired	Action Specifier	Activation Time
		M	T	W	T	F	S	S	H			
1												
2												
3…20												

1. **Enter the schedule number (01-20) and time window number (01-20),** and note the day of the week the action is desired.
2. **Enter the code for the desired action and action specifier.** The action codes represent the events that are to take place when the scheduled time is reached. Each action also requires an action specifier, which defines what the action will affect (relay, relay group, partition, zone list, user group). The action specifier varies, depending on the type of action selected.

   The following is a list of the Action Codes (desired actions) used when programming Time-Driven events. Note that these codes are independent of the relay codes programmed during *Output Programming* in the *#93 Menu Mode*.

Relay Commands

Action Code	Action	Action Specifier
01	Relay On	Relay #
02	Relay Off	Relay #
03	Relay Close for 2 seconds	Relay #
04	Relay Close XX minutes (set in field 1*74)	Relay #
05	Relay Close YY seconds (set in field 1*75)	Relay #
06	Relay Group On	Relay Group #
07	Relay Group Off	Relay Group #
08	Relay Group Close for 2 seconds	Relay Group #
09	Relay Group Close XX minutes (set in field 1*74)	Relay Group #
10	Relay Group Close YY seconds (set in field 1*75)	Relay Group #

Arm/Disarm Commands

Action Code	Action	Action Specifier
20	Arm-STAY	Partition(s)
21	Arm AWAY	Partition(s)
22	Disarm	Partition(s)
23	Force Arm STAY (Auto-bypass faulted zns)	Partition(s)
24	Force Arm AWAY (Auto-bypass faulted zns)	Partition(s)
25	Arm INSTANT	Partition(s)
26	Arm MAXIMUM	Partition(s)

- The auto-arm warning (field 2*06) applies when using Time-Driven events to auto-arm.
- Temporary schedules do not override an auto-arming or auto-disarming programmed in Time-Driven events.
- The auto-arming window cannot be extended using the Installer Code + #82 Mode.

Bypass Commands

Action Code	Action	Action Specifier
30	Auto bypass – Zone list	Zone list #
31	Auto unbypass – Zone list	Zone list #

Open/Close Windows

Action Code	Action	Action Specifier
40	Enable Opening Window by partition	Partition(s)
41	Enable Closing Window by partition	Partition(s)
42	Enable Access Window for access group	Access Group

Access Control Commands

Action Code	Action	Action Specifier
55	Access Point Grant	Access Point #
56	Access Point Grant with Override	Access Point #
57	Access Point Protect	Access Point #
58	Access Point Bypass	Access Point #
59	Access Point Lock	Access Point #
60	Access Point Exit	Access Point #
61	Access Point Group Grant	Group #
62	Access Point Group Grant with Override	Group #
63	Access Point Group Protect	Group #
64	Access Point Group Bypass	Group #
65	Access Point Group Lock	Group #
66	Access Point Group Exit	Group #
67	Access Point Partition Grant	Partition #
68	Access Point Partition Grant with Override	Partition #
69	Access Point Protect by Partition	Partition #
70	Access Point Bypass by Partition	Partition #
71	Access Point Lock by Partition	Partition #
72	Access Point Exit by Partition	Partition #

Action Code	Action	Action Specifier
73	Access Point Trigger On	Trigger #
74	Access Point Trigger Off	Trigger #
77	Access Point Group Enable	Group #
78	Access Point Group Disable	Group #

3. Enter the desired activation time (when the action is to take place). Select from:

Activation Time	Description
1	Beginning of time window.
2	End of time window.
3	During time window active period only (on at beginning of window, off at end). For example, if bypass is selected to activate during the window, zones in a zone list are bypassed at the beginning of the window and unbypassed at the end of the window.
4	Beginning and end of time window (e.g., a coffee break buzzer). In this example, if relay pulse is selected, the relay pulses for 2 seconds at the beginning of the window, signaling the beginning of the coffee break. At the end of the window it pulses again, signaling the end of coffee break.
5	Random time at the start of the time window (occurs within 30 minutes after the start of the time window). **NOTE:** Since the randomization for choice "5" occurs within 30 minutes after the start of the window, the time window must be at least 30 minutes in duration.
6	Random time at the end of the time window (occurs within 30 minutes after the end of the time window).
7	Random during the time window (begins within 30 minutes after the start of the time window and ends within 30 minutes after the end of the time window). **NOTE:** Since the randomization for choice "7" occurs within 30 minutes after the start of the window, the time window must be at least 30 minutes in duration.

Field *04 must be enabled for randomization. A user must initiate a random schedule by entering one of the following sequences:

- **[User Code] + [#] + [41]**. This will randomize, up to 30 minutes, the activation time of all devices, programmed for randomization, assigned to the partition the sequence is entered in. Enter the sequence again to turn off the random schedule.
- **[User Code] + [#] + [42]**. This is the same as the method above, except the randomization occurs only on devices with activation times within 6 PM and 5 AM. Enter the same sequence again to turn off the random schedule.

UL You must not program Random Scheduling of Time Driven Events for UL installations.

Time-Driven Event Programming

The following menu items must first be programmed in *Output Programming in the #93 Menu Mode*:

Enter Relay No.	(reference identification number)
Output Group	(if applicable)
Restriction	
Output Type	(V-Plex, 4204 or X-10)
Zone No.	(V-Plex)
ECP Address	(4204)
Relay No.	(4204)
House Code	(X-10)
Unit Code	(X-10)

After entering Scheduling Menu Mode, press **[0]** until the "Timed Events ?" prompt appears.

PROMPT	EXPLANATION
Timed Events ? 1 = YES 0 = NO 0	Enter **1** to program timed events.
TIMED EVENT # ? 01-20, 00=Quit 01	Enter the timed event number to be programmed **(01-20)**. Press [✳]. The system then prompts the user to enter the desired action to be taken. Enter **00** at the "TIMED EVENT #?" prompt to quit the timed event menus and display the "Quit ?" prompt.
01 ACTION ? none 00	Enter the action code for this timed-event number from the list at the left. This could be an output command, an arming command, or any other Time-Driven event. Press [✳] to accept the entry. The prompt for the action specifier appears.

ACTION CODES	EXPLANATION	ACTION SPECIFIER
01=Relay On 02=Relay Off 03=Relay Close for 2 seconds 04=Relay Close XX minutes 05=Relay Close YY seconds	**Actions 01-05** If you selected actions **01-05**, the prompt at the right appears. Enter the relay number. Press [✳] to accept entry. The "Time Window ?" prompt appears.	01 RELAY # ? 00
06=Relay Group On 07=Relay Group Off 08=Relay Group Close for 2 seconds 09=Relay Group Close XX minutes 10=Relay Group Close YY seconds	**Actions 06-10** **If you selected actions 06-10, the prompt at the right appears. Enter the relay group number.** **Press [✳] to accept entry. The "Time Window ?" prompt appears.**	01 RELAY GRP # ? 00
20=Arm-STAY 21=Arm AWAY 22=Disarm 23=Force Arm STAY 24=Force Arm AWAY 25=Arm INSTANT 26=Arm MAXIMUM 40=Enable Open Window by Part. 41=Enable Close Window by Part.	**Actions 21-26 and 40-41** If you selected actions **21-26** or **40-41**, the prompt at the right appears. Enter the partition to which the action applies. Enter **0** to select all partitions. Enter a partition number again to deselect it. Press [✳] to accept entry. The "Time Window ?" prompt appears.	PART? 12345678 HIT 0-8 X X
30=Auto bypass – Zone list 31=Auto unbypass – Zone list	**Actions 30-31** If you selected actions **30-31**, the prompt at the right appears. Enter the zone list number that contains the zones to be bypassed or unbypassed. Press [✳] to accept entry. The "Time Window ?" prompt appears.	01 ZONE LIST ? ENTER 01-15 01
42=Enable Access Window for Access group(s)	**Action 42** If you selected action **42**, the prompt at the right appears. Enter the group number to which the time window will apply. Press [✳] to accept entry. The "Time Window ?" prompt appears.	GROUP ? 12345678 HIT 0-8 X
55=Access Point Grant 56=Access Point Grant w/Override 57=Access Point Protect 58=Access Point Bypass 59=Access Point Lock 60=Access Point Exit	**Actions 55-60** If you selected actions **55-60**, the prompt at the right appears. Enter the access point number. Press [✳] to accept entry. The "Time Window ?" prompt appears.	01 ACCESS POINT # 000

ACTION CODES	EXPLANATION	ACTION SPECIFIER
61=Access Point Group Grant 62=Access Point Group Grant w/Override 63=Access Point Group Protect 64=Access Point Group Bypass 65=Access Point Group Lock 66=Access Point Group Exit 77=Access Point Group Enable 78=Access Point Group Disable	**Actions 61-66 and 77-78** If you selected actions **61-66**, the prompt at the right appears. Enter the group number. Press [✳] to accept entry. The "Time Window ?" prompt appears.	01 GROUP # 00
67=Access Point Partition Grant 68=Access Point Partition Grant w/Override 69=Access Point Protect by Partition 70=Access Point Bypass by Partition 71=Access Point Lock by Partition 72=Access Point Exit by Partition	**Actions 67-72** If you selected actions **67-72**, the prompt at the right appears. Enter the partition to which the action applies. Enter **0** to select all partitions. Enter a partition number again to deselect it. Press [✳] to accept entry. The "Time Window ?" prompt appears.	PART? 12345678 HIT 0-8 X X
73=Access Point Trigger On 74=Access Point Trigger Off	**Actions 73-74** If actions **73-74** were selected, the prompt at the right will be displayed. Enter the trigger number. Press [✳] to accept entry. The "Time Window ?" prompt appears.	01 TRIGGER # 00

PROMPT	EXPLANATION
01 Time Window ? 00:00 00:00 01	Enter the time window number (**01-20**) for which this timed event is to occur. As the number is keyed in, the actual time that has been stored for the time window number is displayed. Press [✳] to accept entry.
01 Active time ? 0	Enter the activation time from **1-10** (listed below). As the number is keyed in, the activation time is displayed. The choices are: **1:** Trigger at the start of the window. **2:** Trigger at the end of the window. **3:** Take effect only for the duration of the window. **4:** Trigger at both the start and the end of the window. Example: coffee break buzzer. **5:** Random trigger, up to 30 minutes, after the start of the window. **6:** Random trigger, up to 30 minutes, after the end of the window. **7:** Take effect only for the duration of the window, but random start and end the window up to 30 minutes. Press [✳] to accept entry.
Days ? MTWTFSSH Hit 0-8 x x	The system then asks for which days the event is to be activated. Press **0** to toggle all days on or off; or press keys **1-8** to toggle the letter "x" under the day on or off (Monday = 1, Holiday = H = 8). When all entries have been made, the "TIMED EVENT #?" prompt is displayed again. Repeat the procedure for each timed event for the installation.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Bank Safe and Vault

The Bank Safe or Vault should be limited to its own partition where only a Master or Manager code would be allowed to operate (see Section 2 of this Manual - Partitioning). If regular users are enabled there is a way to disable their access (see below):

1. Enter Scheduling Mode by entering Installer Code + [#] + [80].
2. Select Time Windows.
3. Create Time Window 01 as -6:00am-10:00am.
4. Create Time Window 02 as 9:30pm-10:00pm, enter 00* to exit Time Windows.
5. Do not Quit Menu Mode, go to O/C Schedules.
6. Enter Vault Partition #.
7. Assign Window 01 as the OP window and Window 02 as the Cl Window for Monday thru Saturday. Exit Program mode.

Vault Partition

1. Program **2*05** = 00, Auto-Arm Delay (partition-specific) Arm at 10pm.
2. Program **2*06** = 00, Auto-Arm Warning Period (partition-specific) No Warning Period.
3. Program **2*07** = 00, Auto-Disarm Delay (partition-specific) Disarm at 6am.
4. Program **2*08** = 1, Force Arm (partition-specific) Enable.
5. Program **2*10** = 1, Allow Disarming Only During Arm/Disarm Windows (partition-specific).
6. Program **2*11** = 0, Allow Disarm Outside Window if Alarm Occurs.

Panel will arm at 10pm Monday thru Saturday with no warning and Only Master/Manager can disarm between 10pm and 6am**.**

To also Disable the Master/Manager from Disarming between 10pm and 6am All Master/Manager codes will only work between 6am and 10pm Monday thru Saturday. They will not work on Sunday or Holidays.

1. Enter program mode Installers code + #80
2. Enter 'Time Windows' and Create window 03 for 6:00am-10:00pm, enter 00* to exit Time Windows
3. Do not Quit Menu Mode, go to Access Sched.
4. Create Access Sched 01 by assigning Window 03 to A1 Monday thru Saturday. Exit Program mode
5. Assign all Master and Manager Codes to Access Schedule 01 when user codes are assigned.

Open and Closed window can be removed from schedule for Saturday to prevent regular users (if they are enabled for this particular partition) from being able to disarm on Saturday, and window can be removed from Limit Access Group 1 for Saturday to prevent Master/Manager Access on Saturday.

1 Enter program mode Installers code + #80.
2. Go to O/C Schedules.
3. Enter Vault Partition, go to Saturday and enter 00 for OP and CL window.
4. Go to Access Schedules.
5. Enter Schedule 01, go to Saturday and enter 00 for Window A1. exit program mode.

Create selected Holidays in Holiday Programming and assign to all partitions. Holiday window in Open/Close Schedule remains empty to prevent regular users (if they are enabled for this particular partition) from being able to disarm on Holidays, and Limit Access Group 1 Holiday Window can remain empty to prevent Master/Manager Access on Holidays.

1. Enter program mode Installers code + #80.
2. Go to Holidays.
3. Enter Selected Holiday dates.
4. Exit program mode.

Limitation of Access Schedules

Limitation of Access is a means by which a user's access code is limited to working during a certain period of time. The system provides eight Access Schedules, each of which consists of two time windows for each day of the week and two time windows for holidays (typically, one for an opening time window and the second for a closing time window). A user, required to follow a schedule, would be assigned to an access group of the same number (e.g., schedule 1= group 1). The user's access code is assigned to a group when that user is added to the system. If no limitations apply, enter **0**.

Limitation of Access Schedule Worksheet

Enter the appropriate time window numbers for each access schedule.

Acc	Mon		Tues		Wed		Thurs		Fri		Sat		Sun		Hol	
Sch	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2	W1	W2
1																
2																
3…8																

NOTE: The holidays used for the access groups are the same as those defined in the holiday schedule.

Limitation of Access Schedules Programming

To program access schedules enter Scheduling Menu Mode **Installer Code + # 80**. After entering Scheduling Menu Mode, press **[0]** until the "Access Sched. ?" prompt appears.

PROMPT	EXPLANATION
Access Sched. ? 1 = YES 0 = NO 0	Enter **1** to program access schedules.
ACCESS SCHED # ? 01-08, 00 = Quit 01	Enter the access control schedule number between **01** and **08**. Press [✳] to accept entry. Enter **00** at the "Access Sched #?" prompt to quit the access control menus and display the Quit ? prompt.
MON A1 Window 1? 00:00 00:00 00	Enter the first time-window number **(01-20)** for this access schedule for the displayed day. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [✳] to continue.
MON A1 Window 2 ? 00:00 00:00 00	Enter the second time-window number from **01-20** for this access schedule for the displayed day. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [✳] to continue.
TUE A1 Window 1? 00:00 00:00 00	Repeat the procedure for the other days of the week. When the last day of the week has been programmed, the windows for holidays may be entered.
Hol A1 Window 1 ? 00:00 00:00 00	Enter the first time-window number for holidays for this access schedule. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [✳] to continue.
Hol A1 Window 2 ? 00:00 00:00 00	Enter the second time-window number for holidays for this access schedule. As the number is keyed in, the actual time that has been stored for the window is displayed. Press [✳] to continue.
Quit ? 1 = YES 0 = NO 0	Enter **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter **1** to quit Scheduling Menu Mode.

Temporary Schedules

Each partition can be assigned a temporary schedule, which overrides the regular open/close schedule (and the holiday schedule). This schedule takes effect as soon as it is programmed, and remains active for up to one week.

Only users with the authority level of manager or higher can program temporary schedules.

A temporary schedule affects only the partition from which it is entered. Temporary schedules can also be reused at later dates simply by scrolling (pressing [#]) to the "DAYS?" prompt and activating the appropriate days. This should be considered when defining daily time windows.

Temporary Schedule Worksheet

Partition/Windows		Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	**Disarm Window**							
	Start Time HH:MM							
	Stop Time HH:MM							
	Arm Window							
	Start Time HH:MM							
	Stop Time HH:MM							
2…8	**Disarm Window**							
	Start Time HH:MM							
	Stop Time HH:MM							
	Arm Window							
	Start Time HH:MM							
	Stop Time HH:MM							

Temporary Schedules Programming

Enter **User Code + [#] + 81** to enter this mode.

PROMPT	EXPLANATION
Mon DISARM WIND. 00:00AM 00:00AM	This prompt is for entering the start and end times of the disarm (opening) window for Monday. Upon entry of this mode, the cursor is positioned on the tens of hours digit of the start time of the disarm window. Enter the desired hour. Press [✳] to move to the minutes field. The minutes are entered in the same manner. Press [✳] to move to the AM/PM position. Pressing any key in the **0-9** range toggles the AM/PM indication. Repeat the procedure for the stop time entry. Press [✳] to store the entries and move to the arming (closing) window for Monday. Pressing [#] scrolls you through the prompts without making any changes.
Mon ARM WINDOW 00:00AM 00:00AM	This prompt is for entering the start and end times of the arm (closing) window for Monday. The cursor is positioned on the tens of hours digit of the start time of the arm window. Enter the hour. Press [✳] to move to the minutes field. The minutes are entered in the same manner. Press [✳] to move to the AM/PM position. Pressing any key in the **0-9** range toggles the AM/PM indication. Repeat the procedure for the stop time entry. After the windows for that day have been completed, the system prompts for disarm and arm time windows for the next day. Press [#] if no changes are desired.
Tue DISARM WIND. 00:00AM 00:00AM	Repeat the procedure described above for all days of the week. When all the windows for all the days have been completed, the system prompts for which days of the schedule are to be activated.
Days ? MTWTFSS Hit 0-7 x x	This is the prompt that actually activates the temporary schedule. To select the days to be activated, enter **1-7** (Monday = 1). An "X" appears under that day, indicating the temporary schedule for that day is active. Entering a day's number again deactivates that day. Pressing **0** toggles all days on/off. The temporary schedule is in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, but all other entries for the temporary schedule remain programmed. Press [✳] to store the entries or press [#] to exit the Temporary Schedule Entry Mode without making any changes.

User Scheduling Menu Mode

The system provides up to 20 "timers" available to the end user to control output devices. The output devices themselves are programmed into the system by the installer during *Output Programming* in the *#93 Menu Mode*. The end user needs only to know the output device number and its alpha descriptor.

The installer may set certain outputs to be "restricted" during *Output Programming* (this prevents the end user from controlling doors, pumps, bell outputs, etc.)

To enter this mode, the user enters **User Code + [#] + 83.**

PROMPT	EXPLANATION
Output Timer # ? 01-20, 00=Quit 01	Enter the output timer number to be programmed **(01-20)**. Press [✳] to accept entry and move to the next prompt. Enter **00** to quit and return to normal operating mode.
06 07:00P 11:45P PORCH LITE 04	If that timer number has already been programmed, a summary screen appears. In this example: 06 = Timer # 07:00PM = Start Time 11:45PM = Stop Time PORCH LITE = Descriptor for Output Device # 4 04 = Output Device # affected by this timer Press [✳] to continue.
06 ENTER OUTPUT# PORCH LITE 04	Enter the desired output number **(01-96)**. As the number is entered, the descriptor for that output device is displayed. Press [✳] to continue.

Entering **00** as the output number deletes the timer (Timer 06, in this example) and displays an output descriptor of "None." Output devices are programmed via #93 Menu Mode.

PROMPT	EXPLANATION
06 ON TIME ? 07:00 PM	The cursor is positioned on the tens of hours digit of the ON time. Enter the desired hour. Press [✳] to move to the minutes field. The minutes are entered in the same manner. The AM/PM indication is toggled by hitting any key from **0-9** while the cursor is under the AM/PM position. Press [✳] to continue.
06 OFF TIME ? 11:45 PM	The cursor positioned on the tens of hours digit of the OFF time. Enter the desired hour. Press [✳] to move to the minutes field. The minutes are entered in the same manner. The AM/PM indication is toggled by hitting any key in the **0-9** range while the cursor is under the AM/PM position. Press [✳] to continue.
06 DAYS? MTWTFSS HIT 0-7 x x	To select the days to be activated, enter **1-7** (Monday = 1). An "x" appears under that day, indicating the output for that day is active. Entering a day's number again deactivates that day. Pressing **0** toggles all days on/off. The outputs are in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, unless the permanent option is selected (next screen prompt). When completed, press [✳] to continue.
06 Permanent ? 0 = NO,1 = YES 0	Selecting "Permanent" **(1)** means that this schedule will be in effect on a continuous basis. Selecting **0** means that this schedule will be in effect for one week only. The letter "x" under the day is then cleared, but all other entries for the output device remain programmed. Press [✳] to accept entry. The system quits User Scheduling Mode and returns to normal operating mode.

Downloading Primer

(Remote Downloading is not a UL Listed feature)

General Information

Downloading allows the operator to remotely access, program, and control the security system over normal telephone lines, IP, or GSM Communicators. Anything that can be done directly from the keypad can be done remotely, using ADEMCO's COMPASS downloading software. To communicate with the control panel, the following is required:

1. IBM PC-compatible 486 33MHz PC or better with 100 MB of available hard disk space and at least 8MB of RAM (12MB is preferred). Windows 3.X, Windows 95, 98, or Windows NT.

Phone Line Up Load/ Downloading

1. One of the following modems:
   - ADEMCO CIA
   - Hayes Smartmodem 1200 (external: level 1.2 or higher; internal: level 1.1 or higher)
   - Hayes Optima 24 + Fax 96 external
   - Hayes Optima 336
   - BizComp Intellimodem 1200 w/volume
   - BizComp Intellimodem 2400

   Other brands are not compatible, even if claimed to be 100% compatible.

Internal modems must have a 4-position DIP switch. Modems with a 6-position DIP switch will not work.

2. Compass revision 1.5.8 or above.

IP/GSM Downloading

Panels can be downloaded via the ECP bus over the following Communicators:

- 7845GSM
- 7845iGSM
- 7845i-ent
- 7720PLUS
- 7720ULFPLUS

Access Security

The following four levels of protection guard the control against compromise while it is being accessed from a remote location:

1. Security code handshake: The subscriber's account number as well as an 8-digit ID number (known only to the office) must be matched between the control and computer.
2. Hang-up and callback: The control panel "hangs up" and calls the computer back at the pre-programmed number only if the security codes match.
3. Data encryption: All data that is exchanged between the computer and control is encrypted to reduce the possibility of anyone "tapping" the line and corrupting data.
4. Operator access levels: Operators may be assigned various levels of access to the downloader, each having its own log-on code. The access levels allow the operators read/write capabilities of the customers' account information. For a detailed explanation of the access levels, see the downloading software User Manual.

NOTES:

- Each time the control panel is accessed successfully, a Callback Requested report is sent to the central station, if Opening reports are programmed.
- When the system is downloading, the keypad displays "MODEM COMM."
- After each download or save an automatic time stamp is done, to indicate the last download (or save) and the operator ID number.
- A complete hard copy of each individual account can be obtained by connecting a printer to the computer. Refer to your computer Owner's Manual or contact your dealer for printer recommendations.

Getting On-Line with a Control Panel

At the protected premises, the control panel must be connected to the existing telephone line (refer to *SECTION 3: Installing the Control*). No programming of the panel is required before downloading to an initial installation.

When establishing a connection between the computer and the control panel, the following occurs:

Stage	What Happens
1	The computer calls up the control panel. (The phone number for each customer must be entered into the customer's account file on the computer.)
2	The control panel answers the phone call at the pre-programmed ring count and executes a handshake with the computer.
3	The computer sends a request for callback to the control, unless callback is not required.
4	The panel acknowledges the request and hangs up. During the next few seconds, the control processes the request, making sure certain encrypted information received from the computer matches its own memory.
5	Upon a successful match, the control panel seizes the phone line and calls the computer back, unless callback is not required. (The phone number to which the computer's modem is connected must be programmed into the control field ✳35.)
6	The computer answers, usually by the second ring, and executes a handshake with the panel.
7	The panel then sends other default information to the computer. If this information matches the computer's information, a successful link is established. The system is now "on-line" with the computer.

- Alarms and Trouble responses and reports are disabled during actual uploading or downloading sessions. If you are on-line, but not actively uploading or downloading, all alarms report immediately. All other reports are delayed until you complete the session.
- The keypads remain active when on-line with a control, but are inactive during actual uploading or downloading sessions.

To download a control without programming any information, perform the following steps:

Step	Action
1	Enter the **Installer Code + [#] + [5]**. The panel temporarily enables a ring count of 5 and sets the Download Callback option to "1" (callback not required).
2	From the computer, call the panel using the downloader software set to "First Communication" Mode. The downloader establishes a session with no callback. The panel information can then be downloaded.

On-Line Control Functions

The following functions can be performed while on-line with a control panel (see field *37):

- Arm the system in the AWAY Mode; disarm the system
- Bypass a zone
- Force the system to accept a new program download
- Shut down communication (dialer) functions (for nonpayment of monitoring fees in an owned system)
- Shut down all security system functions (for nonpayment for a leased system)
- Inhibit local keypad programming (prevents takeover of your accounts)
- Leave a message for customer

  NOTE: Messages sent to the control panel from the downloader will be viewable at ALL partitions.
- Command the system to upload a copy of its resident program to the office
- Read: arming status, AC power status, list of faulted zones, list of bypassed zones, 1000 event log, list of zones currently in alarm, list of zones currently in trouble, and ECP equipment list
- Set the real-time clock

Telco Handoff

Telco handoff is another method of getting on-line with the downloader. The installer or customer enters the **User Code + [#] + [1]**, while on the phone line with the computer's modem phone line. The customer will get cut-off and the panel and download computer will establish a connection.

Setting the Real-Time Clock

General Information

This system provides a real-time clock, which must be set in order for the system's event log to keep track of events by time and date. It must also be set in order to execute scheduling programs (Time-Driven events).

Use a 6160 alpha keypad to set the real-time clock, or set the clock via the downloader software. Only users with Installer or Master authority level can set the clock.

Setting the Time and Date

To set the real time clock, perform the following steps:

Step	Action
1	Enter Installer or Master Code + [**#**] **63**. Typical display shows: TIME/DATE — THU 12:01 AM 01/01/90 The day of the week is automatically calculated based on the date entered. Time and date entries are made by simply entering the appropriate hour, minute, month, day and year. Press [✳] to move the cursor to the right of the display, to the next position. Press [#] to move the cursor to the left of the display, to the previous position.
2	Enter the correct hour. Then press [✳] to move to the "minutes" field.
3	Enter the correct minutes. Press [✳] to move to the AM/PM position.
4	Press any key 0-9 to change AM to PM, or PM to AM. Press [✳] to move cursor to the "month" field position.
5	Enter the correct month using a 2-digit entry. Press [✳] to move cursor to the "day" field position.
6	Enter the correct day using a 2-digit entry. Press [✳] to move cursor to the "year" field position.
7	Enter the correct year. Press [✳] to exit the real-time clock edit mode.

User Access Codes

General Information

The VISTA-128BPT allows a total of 150 security access codes to be allocated. The VISTA-250BPT allows a total of 250 security access codes to be allocated. Each security access code is identified by a user ID number. **Regardless of the number of partitions each code has access to, it occupies only one user slot in the system. If a code is not used in all partitions, that user ID number cannot be used again.**

The Quick Arm feature can also be programmed (partition-specific program field *29). The Quick Arm feature allows the user to arm the system by pressing the [#] key instead of the security code. The security code must always be entered to disarm the system.

A user code other than the installer code must be programmed in order for the Quick Arm feature to function.

The system is shipped with the following defaults for the user codes:

User	4-Digit Code	Alpha Descriptor
User 1 (Installer)	4140	INSTLR
User 2	1234	MASTER

User Codes & Levels of Authority

Each user of the system can be assigned a level of authority, which authorizes the user for certain system functions. A user can have different levels of authority within different partitions

Use the "View Capabilities" keypad function (**User Code + [✳] + [✳])** to view the partitions and authority levels for which a particular user is authorized. These levels are described below.

Level 0: Installer (User 1) Code

- Programmed in field *00 (default = 4-1-4-0). Installer Open/Close reporting selected in field *39.
- Can perform all system functions (arm, disarm, bypass, etc.), but **cannot disarm** if armed by another code (or by Quick Arm).
- Can add, delete, or change all other codes, and can select Open/Close reports for any user.
- Is the only code that can be used to enter program mode. The Installer Code can be prevented from re-entering the Program Mode by exiting using ✳98.
- Must program at least one Master Code during initial installation. Master Codes are codes intended for use by the primary user(s) of the system.

Level 1: Master Codes

- Can perform all normal system functions.
- Can be used to assign up to 148 lower-level codes, which can be used by other users of the system.
- Cannot assign anybody a level of 0 or 1.
- May change own code.
- Can add, delete, or change Manager or Operator Codes. Each user's code can be individually eliminated or changed at any time.
- Open/Close reporting is automatically the **same** as that of the Master who is adding the new user.

Level 2: Manager Codes

- Can perform all system functions (arm, disarm, bypass, etc.) programmed by Master.
- May add, delete, or change other users of the system below this level (Manager cannot assign anybody a level of 0, 1, or 2).
- May change own code.
- Open/Close reporting is automatically the **same** as that of the Manager who is adding the new user.

Levels 3-5: Operator Codes

- Can operate a partition, but cannot add or modify any user code (see table below).

Level	Title	Functions Permitted
3	Operator A	Arm, Disarm, Bypass
4	Operator B	Arm, Disarm
5	Operator C	Arm, Disarm only if armed with same code

- Operator C (sometimes known as the Babysitter Code) cannot disarm the system **unless** the system was armed with that code. This code is usually assigned to persons who may need to arm and disarm the system at specific times only (e.g., a babysitter needs to control the system only when babysitting).

Level 6: Duress Codes

- Sends a silent alarm to a central monitoring station if the user is being forced to disarm (or arm) the system under threat (system must be connected to a central station).
- When the system's Auxiliary Voltage Triggers are connected to another communication's media (Derived Channel/Communicator), note that duress is signaled on the same trigger that signals silent panic (whereas duress has its own unique report when digitally communicated).
- Assigned on a partition-by-partition basis, and can be any code or codes desired.

General Rules on Authority Levels and Changes

The following rules apply to users when making modifications within the system based on the user code authority levels:

- Master Codes and all lower-level codes can be used interchangeably when performing system functions within a partition (a system armed with a user's temporary code can be disarmed with the Master Code or another user's temporary code), except the Operator Level C Code described above.
- A user may not delete or change the user code of the SAME or HIGHER authority than that which he is assigned.
- A user (levels 0, 1 and 2 only) may only ADD users to a LOWER authority level.
- A user may assign other users access to only those partitions to which he himself has access.
- A user code can be DELETED or CHANGED only from within the partition it was created in.
- User numbers must be entered in 3 digits. Single-digit user numbers must, therefore, always be preceded by a "00" (e.g., 003, 004, 005, etc.). Make sure the end user understands this requirement. Temporary codes are entered as 4-digit numbers.

Duress Reporting **NOTE:** A non-zero report code for zone 992 (duress) must be programmed, and partition-specific field *85 duress location enabled, to enable Duress reporting.

- The Duress report-triggering logic activates on the 5th key depression (such as OFF), not the 4th key depression (last digit of code). Duress reports are not triggered if the 5th key is a [*], such as when you perform a GOTO or view the capabilities of a user.

Open/Close Reporting Note: When a user is added, the system prompts for Open/Close reporting capability only if the installer is adding the new user. When a Master or Manager adds a new user, the new user's Open/Close reporting is the same as that of the Master or Manager who is adding the user. If Open/Close reports are required to be selectable by the Master or Manager, the Installer should assign two Master or Manager user codes: one with Open/Close reporting enabled, and one without.

Note that Open/Close reporting of Quick Arm is enabled if User 002 is enabled for Open/Close reporting, and that Quick Arm reports as User 000. In order for Quick Arm reports to be sent for all partitions, User 002 must have authority and Open/Close must be enabled for all partitions. If a code with access to all partitions is not desired, it is suggested that user 002 be assigned authority level 5 in all partitions, and that the code be kept secret. Authority level 5 cannot disarm the system unless armed by that user.

ADEMCO Contact ID format is capable of reporting Users 001-150 uniquely. If any other report format is used, only user numbers 001 – 015 can uniquely report to the central station. Users 016 – 150 will report as User 015.

Multiple Partition Access

Each user is programmed for a primary (home) partition. A user can also be given access to operate one or more additional partitions. Within each partition, each user may be programmed to have different levels of authority. For example, User 003, the VP of Engineering, could be assigned to work within the Engineering Department (Partition 1) of ABC Manufacturing. Because he needs the full capabilities in his area, he is assigned as a MASTER with Level 1 authority.

He must also be able to gain access to the manufacturing area (Partition 2) on an emergency basis. You can set this up easily by requesting that he also be assigned to Partition 2, with a level of authority set lower, such as Level 4 (OPERATOR Level B).

The control automatically assigns him the same user number within Partition 2.

EXAMPLE OF MULTIPLE PARTITION ACCESS

Part 1	Part 2	Part 3	Part 4	Part 5	Part 6	Part 7	Part 8
User 3	User 3						
Level 1	Level 4						
Master	Oper B						

In the above example, User 3 has MASTER authority in Partition 1 and OPERATOR B authority in Partition 2. His user number is the same for both partitions. Note that if a user number is already being used in a partition, the system will automatically assign a new user an unused number. Also notice that no access is allowed for this user into Partitions 3 – 8. Attempts to access these partitions would be denied automatically.

Adding a Master, Manager, or Operator Code

During user code entry, normal key depressions at other keypads in a partition are ignored. However, panic key depression causes an alarm and terminates user entry.

Enter **Installer Code†+ [8] + new user no. (002-250) + new user's code**

†Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g., a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code). Keypad prompts for the authority level for this user.

NOTE: All references to the number of user codes pertain to the VISTA-250BPT. The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
User Number = 003 Enter Auth. Level	Enter the level number as follows: 1 = Master 2 = Manager 3 = Operator Level A 4 = Operator Level B 5 = Operator Level C 6 = Duress Keypad then prompts for Open/Close reporting option for this user.
Open/Close Rep.? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether or not arming/disarming by this user will trigger Opening and Closing reports. This prompt appears only if the Installer Code is used to add a user.
Group Bypassing? 0 = NO , 1 = YES	Enter 1 (YES) to allow this user to perform group bypasses. Enter 0 (NO) this user will not be able to perform group bypasses. **NOTE:** In addition to enabling the user for group bypassing, the user **must also have access to the partition(s) containing the zones being bypassed and have global arming capability**.
Access Group? Enter 0-8	If access schedules have been programmed, this prompt appears. Enter the user's access group number (1-8) if this user should have limited access to the system. Enter **0** if no access group should be assigned.
RF Button ? 0=NO , 1=YES	If a 5800 Series button transmitter has been enabled for arming/disarming functions, and is not assigned to a user, this prompt appears. Press **0** (NO) or **1** (YES).
Enter Button ZN # (001-087)	If you answered "yes" to the RF button question, the zone number for the button is requested. Enter any one of the zone numbers assigned to the button transmitter as AWAY, STAY, or DISARM. The system then assigns **all** buttons of the transmitter to this user number.
Multi-Access ? 0 = NO , 1 = YES	Press **0** (NO) if the user is to have access to this partition only. Press **1** (YES) if the user is to have access to more than one partition. If NO, the program exits this mode. If YES, the keypad prompts for the Global Arm option for this user.
Global Arm ? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether this user will be allowed to arm more than one partition via Global Arm prompts. The keypad now prompts for the user's access to the next partition.
Part. 2 – SHOP ? 0 = NO , 1 = YES	Press **0** (NO) or **1** (YES), depending on whether this user will have access to the displayed partition number. If NO, the keypad displays this prompt for the next partition number in sequence. If YES, the keypad prompts for the following: • User's authority level in the displayed partition (see Authority Level prompt above). • Open/Close option for this user in the displayed partition (see Open/Close prompt above). • Global Arm option for this user in the displayed partition. When all partitions have been displayed, the keypad will scroll through all partitions to which access has been assigned, and will display the user number, authority level, open/close and global arm options that were programmed for each partition to which the user was granted access.
Part. 1 A0* WHSE User 003 Auth=3G.	Note that the "G" following the authority level indicates that the global arm feature is enabled for this user in the displayed partition, and that the period at the end of the second line indicates Open/Close reporting is enabled for this user in the displayed partition. The [T] indicates the partition from which the user may be changed or deleted.

Changing a Master, Manager, or Operator Code

Enter **Installer Code*+ [8] + new user no. (002-250) + new user's code**

*Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g. a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code).

NOTE: The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
User Number = 003 ADD NEW USER?	The system detects that the user number is already assigned, and prompts if this is a new user. Press **0** (NO). The system then confirms that the change is allowed based on authorization level.

Adding an RF Key to an Existing User

To add an RF key to an existing user, or to change a user's global arm option, first delete that user's code, then re-add the user code as described in the "Adding a Master, Manager, or Operator Code" paragraph.

Deleting a Master, Manager, or Operator Code

Enter **your code*+ [8] + new user no. (002-150) + your code again**

*Or Master or Manager Code, but the code must be a higher level of authority than the code being changed (e.g. a Manager Code can add an Operator-level Code, but cannot add a Master or another Manager Code).

NOTE: The VISTA-128BPT allows only 150 user codes.

PROMPT	EXPLANATION
OK TO DELETE 003? 0=NO 1=YES	The system prompts to confirm that you want to delete this user. Press **0** (NO) or **1** (YES). If you answered "yes," that user's code is removed from all partitions to which it was assigned, and all authorization levels and other information about that user are deleted. Note that a user can be deleted only by a user with a higher authority level. A user cannot delete himself.

A user code can be deleted only from the partition through which it was entered. If an attempt is made to delete from another partition, the message "User [XXX] Not Deleted" is displayed.

Exiting the User Edit Mode

Press either [T] or [#], or don't press any key for 10 seconds.

Testing the System

Battery Test

When AC power is present, the VISTA-128BPT/VISTA-250BPT runs a brief battery test every 60 seconds to determine if there is a battery connected, and runs an extended battery test every 4 hours to check on the battery's condition.

If the VISTA-128BPT/VISTA-250BPT finds that the battery voltage is low (less than approximately 11.5V), it initiates a keypad "SYSTEM LOBAT" display and a rapid keypad beeping sound. It also sends a Low Battery report to the central station (if programmed). The keypad is cleared by entering any security code + OFF, and a Restore report is sent to the central station if the situation has been corrected.

Dialer Test

The VISTA-128BPT/VISTA-250BPT may be programmed to automatically transmit test reports to a central station at intervals ranging from once per hour to once per 9999 hours (field ✳27).

UL requires the test report to be transmitted at least once every 24 hours. The system can be programmed to send the first report at any time of the day, or on any day of the week (field ✳83).

Burglary Walk-Test (Code + [5] TEST)

This test causes the system to sound keypad beeps in response to faults on zones for the purpose of allowing proper zone operation to be checked without triggering alarms. This test can be activated by any-level user by entering the corresponding security code and pressing TEST while the burglary portion of the system is disarmed. UL requires that this test be conducted on a weekly basis.

When this test is first entered, the system activates the alarm output for 3 seconds. The system sends a Start of Walk-Test message to the central station. The keypad displays "Burg Walk Test in Progress" and sounds a single beep every 15 seconds while the test remains active.

Open and close each protected door and window in turn. Each action should produce three beeps from the keypad. Walk in front of any motion detectors. Listen for three beeps when the detector senses movement.

The keypad displays the zone number and alpha descriptor while a door or window remains open or while a detector remains activated.

To end this test, enter any security code and press OFF. An End of Walk-Test message is sent to the central station.

The system automatically exits the Test mode if there is no activity (no doors or windows are opened and closed, no motion detectors are activated, etc.) for 30 minutes on the VISTA-128BPT, 60 minutes on the VISTA-250BPT. The system beeps the keypad(s) twice every 15 seconds during the last 5 minutes as a warning that it is about to exit the Test mode and return to normal operation.

Armed Burglary System Test

Alarm messages are sent to the central station during the armed system tests. Notify the central station that a test will be in progress.

A display of "COMM. FAILURE" indicates a failure to communicate (no kissoff by the receiver at the central station after the maximum number of transmission attempts is tried). If this occurs, verify that the phone line is connected, the correct report format is programmed, etc.

To perform an armed burglary test, proceed as follows:

Step	Action
1	Notify the central station that a test of the system is being performed.
2	Arm the system.
3	Fault one or more zones.
4	Silence alarm sounder(s) each time by entering the code and pressing OFF. **NOTE:** The system must be rearmed after each code + off sequence.
5	Check that entry/exit delay zones provide the assigned delay times.
6	Check the keypad-initiated alarms, if programmed, by pressing the panic key pairs (✳ and #, 1 and ✳, and/or 3 and #). The word ALARM and a descriptor "999" are displayed for ✳ and #. If [1] and [✳] are pressed, "995" is displayed; if [3] and [#] are pressed, "996" is displayed.
7	If the system has been programmed for audible emergency, the keypad emits a loud, steady alarm sound. Silence the alarm by entering the security code and pressing OFF. If the system has been programmed for silent panic, there are no audible alarms or displays. A report is sent to the central station, however.
8	Notify the central station that all tests are finished, and verify results with them.

Testing Wireless Transmitters

Transmitter ID Sniffer Mode

Use the Transmitter Sniffer Mode to test that transmitters have all been properly programmed.

If a transmitter does not have its serial number "enrolled," it will not turn off its zone number.

To enter the Transmitter ID Sniffer Mode, proceed as follows:

Step	Action
1	Enter **Installer Code + [#] + [3].** The keypad displays all zone numbers of wireless units programmed into the system.
2	Fault each wireless zone, causing each device to transmit. As the system receives a signal from each of the transmitters, the zone number of that transmitter disappears from the display.
3	Enter **Installer Code + OFF** to exit the Sniffer Mode.

Go/No Go Test Mode

Checking the transmitters in this mode assists in determining good mounting locations, and verifies that the RF transmission has sufficient signal amplitude margin for the installed system.

- All partitions containing wireless transmitters must be placed in the test mode for sensitivity reduction of the RF receiver (50% sensitivity). Otherwise, the RF receiver remains at full strength.
- Make sure that all partitions are disarmed when performing this test, as the wireless receiver gain is reduced in half.

To enter the Go/No Go Test Mode, proceed as follows:

Step	Action
1	Enter **Installer Code + [5].**
2	Fault each wireless transmitter, causing each device to transmit. **NOTE:** If a single receiver is used, the keypad beeps three times to indicate signal reception. If two receivers are used, the keypad beeps once if the first receiver received the signal, twice if the second receiver received the signal, and three times if both receivers heard the signal.
3	If the keypad does not beep, reorient or move the transmitter to another location. Usually a few inches in either direction is all that is required.
4	Enter **Installer Code + OFF** to exit the Go/No Go Test Mode.

Smoke Detector Test

All smoke detectors must be tested monthly by pressing the TEST button located on the detector. If the TEST button does not cause the detector to activate it must be replaced immediately.

Trouble Conditions

Check or Trouble Messages

Display	Description
CHECK or TRBL (as per field 1✳07)	This indicates that a problem exists on the zone number displayed. Zone trouble may be caused by one of the following conditions: • A hardwired fire zone is open (broken wire). • A Day/Night zone (zone type 5) is faulted. • A polling loop zone is not seen by the control panel. • A polling loop zone has been tampered (cover removed on a 4190). • A wireless zone has not checked in during the time programmed in field 1✳31. • A 5800 Series transmitter has been tampered (cover removed).
CHECK 8XX XX = 00-30	This indicates a trouble on a peripheral device (connected to the panel's keypad terminals) of the corresponding device address (00-30).
CHECK 9XX XX = 00-99	This indicates that a system trouble exists (RF receiver, bell output, etc.).

If the problem has been corrected, enter an OFF sequence (**Security Code + OFF**) twice to clear the display.

Power Failure

Display	Description
AC LOSS POWER LED is off	This indicates that the system is operating on battery power only. Check to see that the circuit breaker for the branch circuit that your system's transformer is wired to has not been accidentally turned off. **Instruct the user to call a service representative immediately if AC power cannot be restored.**

Other System Messages

Display	Description
COMM FAILURE	This indicates that a failure occurred in the telephone communication portion of your system.
LO BAT	This indicates that a low-battery condition exists in the wireless transmitter displayed. Pressing any key silences the audible warning sound.
SYSTEM LO BAT	This indicates that a low-battery condition exists with the system's backup battery.
RCVR SETUP ERROR	This indicates that the system has more wireless zones programmed than the wireless receiver can support. If this is not corrected, none of the zones in the system will be protected. If additional wireless zones are desired, use an appropriate receiver.
MODEM COMM	This indicates that the control is on-line with a remote computer.

To the Installer

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.

The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Turning the System over to the User

Fully explain the operation of the system to the user by going over each of its functions, as well as the User Guide supplied.

In particular, explain the operation of each zone (entry/exit, perimeter, interior, fire, etc.). Be sure the user understands how to operate any emergency feature(s) programmed into the system.

Contacting Technical Support

PLEASE, before you call Technical Support, be sure you:

- READ THE INSTRUCTIONS!
- Check all wiring connections.
- Determine that the power supply and/or backup battery are supplying proper voltages.
- Verify your programming information where applicable.
- Verify that all keypads and devices are addressed properly.
- Note the proper model number of this product, and the version level (if known) along with any documentation that came with the product.
- Note your Honeywell customer number and/or company name.

Having this information handy will make it easier for us to serve you quickly and effectively.

Technical Support:	1-800-645-7492 (8 a.m.-8 p.m. EST)
World Wide Web Address:	http://www.security.honeywell.com

Regulatory Agency Statements

UL Installation Requirements

The following requirements apply to both UL Residential and UL Commercial Burglary installations:

- All partitions must be owned and managed by the same person(s).
- All partitions must be part of one building at one street address.
- The audible alarm device(s) must be placed where it/they can be heard by all partitions.
- The control cabinet must be protected from unauthorized access. This can be done by installing a tamper switch on the cabinet door (not supplied with VISTA-128BPT/VISTA-250BPT) or by installing a UL Listed passive infrared detector positioned to detect cabinet access. Wire the selected device to any EOLR-supervised zone (Zone 1-8). Program this zone for day trouble/night alarm (type 05) or 24-hour audible alarm (type 07) response. The 24-hour alarm response must be used for multiple-partitioned systems.
- Remote downloading and auto-disarming are not UL Listed features.

NOTE: UL Commercial Burglary installations require the attack resistant cabinet. The cabinet is included in the VISTA-ULKT kit.

UL609 Local Mercantile Premises/Local Mercantile Safe & Vault

Use the following guidelines for a Local Mercantile Premises/Local Mercantile Safe & Vault installation:

- All zones must be configured for EOLR supervision (✳41=0). Wireless sensors may not be used. If 4190WH V-Plexs are used set field ✳24 to "0" to enable tamper detection.
- Attach a door tamper switch (supplied) to the VISTA-128BPT/VISTA-250BPT cabinet backbox. For safe and vault installations, a shock sensor (not supplied) must also be attached to the backbox. (Also see *SECTION 3: Installing the Control*)
- Wire an ADEMCO AB12M Bell/Box to the bell output. Bell wires must be run in conduit. Program the bell output for a timeout of 16 minutes or longer timeout and for confirmation of arming ding. (Also see *SECTION 3: Installing the Control*.)
- Wire the VISTA-128BPT/VISTA-250BPT tamper switch and AB12M Bell/Box tamper switches to any EOLR-supervised zone (zones 1-8). Program this zone for day trouble/night alarm (type 05) or 24-hour audible alarm (type 07) response. The 24-hour alarm response must be used for multiple-partitioned systems.
- Entry delays must not exceed 45 seconds, and exit delays must not exceed 60 seconds.

UL365/UL609 Bank Safe and Vault Alarm System

- Follow the instructions for UL609 local installations above and Bank/Mercantile Safe and Vault (page 3-2) sections of this manual.
- Bell 1 Confirmation of Arming Ding (*16) must be set to 1 to on (enabled) (will automatically test bell).
- Entry delays or any other delays to report alarms may not exceed 45 seconds.
- Models 7845i-ent, 7845i-GSM
- Bell Timeout must be programmed for 16 minutes min. (See Section 5, page 5-2)
- Two 17.2AH Batteries must be used for this application.
- The main protective circuits, linings and attachments on the safe and vault, control units and alarm housing must be of the normally closed circuit, fully supervised type.
- To be installed inside the safe or vault.

UL365 Police Station Connected Burglar Alarm

Follow the instructions for UL609 local installations given above.

For Systems without Line Security:

- You may use the VISTA-128BPT/VISTA-250BPT dialer alone, or the 7845i-ent Communicator alone.
- When using the dialer, program it to send Burglary Alarm, Low Battery, and Communicator Test reports. Field ✳27 must be set to "0024" (or less).
- If you are using the 7845i-ent Communicator, connect it to the VISTA-128BPT/VISTA-250BPT burglary/audible panic alarm trigger.

For Systems with Line Security:

- You must use a GSMHS Communicator.

UL611/UL1610 Central Station Burglary Alarm

Follow the instructions for UL609 Local installations given above.

For Systems without Line Security:

- You must use the VISTA-128BPT/VISTA-250BPT' dialer with a 7845i-ent Communicator.
- Connect the control's burglary/audible panic alarm trigger (on J7 header) and the 659EN's phone line monitor output to the 7845i-ent. The 7845i-ent will send a report to the central station when a telephone line fault condition is detected.
- Also connect the 7845i-ent Communicator's fault output to one of the VISTA-128BPT/VISTA-250BPT' EOLR-supervised zones (i.e., 1-8). Program this zone for a trouble by day/alarm by night (type 05) or a 24-hour alarm (type 07, 08) response to communicator's faults.
- Program the control's dialer to send Burglary Alarm, Trouble, Opening/Closing, and Low Battery reports.

For Systems with Line Security:

Follow the instructions for Systems without Line Security, except use the GSMHS Communicator in place of the 7845i-ent.

California State Fire Marshal (CSFM) and UL Residential Fire Battery Backup Requirements

The California State Fire Marshal and UL have regulations that require all residential fire alarm control panels to have backup battery with sufficient capacity to operate the panel and its attached peripheral devices for 24 hours in the intended standby condition, followed by at least 4 minutes in the intended fire alarm signaling condition.

The VISTA-128BPT/VISTA-250BPT can meet this requirement without using a supplemental power supply, provided that the panel's outputs (including the current drawn from the auxiliary power output terminals) are limited as shown below:

- Output current is limited to 750mA maximum total auxiliary power, polling loop, and bell output current.
- Maximum auxiliary current is 300mA (including polling loop current).
- A 14AH battery is used. (Yuasa model NP7-12 recommended; use two connected in parallel.) A dual-battery harness is provided with ADEMCO No. 4100EOLR Resistor Kit (kit also contains EOL resistors having spade lug/heat shrink tubing construction approved by UL and CSFM for fire zone usage). Both batteries fit inside the panel's cabinet.

ULC Installation Requirements

- The zone inputs of the control unit are considered Low Risk applications only.
- The control unit must not be mounted on the exterior of a vault, safe or stockroom.
- Subscriber control units capable of maintaining opening (disarming) and closing (arming) schedules must facilitate a hardcopy printout of the opening (disarming) and closing (arming) schedule programming and of all the programmed holidays.
- Telephone service must be of the type that provides for timed release disconnect.
- A server employed for control over network addressing, encryption or re-transmission, Must be designed to remain in the "on state" at all times.
- Encryption must be enabled at all times for active communications channel security.
- For ULC Installations, refer to CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults; CAN/ULC-S301, Standard for Central and Monitoring Station Burglar Alarm systems and CSA 22.1, Canadian Electrical Code, Part I, Safety Standard for Electrical Installations.

FEDERAL COMMUNICATIONS COMMISSION (FCC) STATEMENTS

The user shall not make any changes or modifications to the equipment unless authorized by the Installation Instructions or User's Manual. Unauthorized changes or modifications could void the user's authority to operate the equipment.

CLASS B DIGITAL DEVICE STATEMENT

NOTE: This equipment has been 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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

INDUSTRY CANADA (IC) STATEMENTS

This device complies with RSS210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

IN THE EVENT OF TELEPHONE OPERATIONAL PROBLEMS

In the event of telephone operational problems, disconnect the control panel by removing the plug from the RJ31X (CA38A in Canada) wall jack. We recommend that you demonstrate disconnecting the phones on installation of the system. Do not disconnect the phone connection inside the control panel. Doing so will result in the loss of your phone lines. If the regular phone works correctly after the control panel has been disconnected from the phone lines, the control panel has a problem and should be returned for repair. If upon disconnection of the control panel, there is still a problem on the line, notify the telephone company that it has a problem and request prompt repair service. The user may not under any circumstances (in or out of warranty) attempt any service or repairs to the system. It must be returned to the factory or an authorized service agency for all repairs.

FCC PART 68 NOTICE

This equipment complies with Part 68 of the FCC rules. On the front cover of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

This equipment uses the following jacks:

An RJ31X is used to connect this equipment to the telephone network.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact the manufacturer for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request that you remove the equipment from the network until the problem is resolved.

There are no user serviceable components in this product, and all necessary repairs must be made by the manufacturer. Other repair methods may invalidate the FCC registration on this product.

This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

This equipment is hearing-aid compatible.

When programming or making test calls to an emergency number, briefly explain to the dispatcher the reason for the call. Perform such activities in the off-peak hours, such as early morning or late evening.

CANADIAN EMISSIONS STATEMENTS

This Class B digital apparatus complies with Canadian ICES-003

NOTICE

The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may cause the telecommunications company to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact an appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The **Ringer Equivalence Number** (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

AVIS

L'étiquette d'Industrie Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme aux normes de protection, d'exploitation et de sécurité des réseaux de télécommunications, comme le prescrivent les documents concernant les exigences techniques relatives au matériel terminal. Le Ministère n'assure toutefois pas que le matériel fonctionnera à la satisfaction de l'utilisateur. Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'enterprise locale de télécommunication. Le matériel doit également être installé en suivant une méthode acceptée da raccordement. L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empêche pas la dégradation du service dans certaines situations.

Les réparations de matériel nomologué doivent être coordonnées par un représentant désigné par le fournisseur. L'entreprise de télécommunications peut demander à l'utilisateur da débrancher un appareil à la suite de réparations ou de modifications effectuées par l'utilisateur ou à cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise à la terre de la source d'energie électrique, de lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

Avertissement : L'utilisateur ne doit pas tenter de faire ces raccordements lui-même; il doit avoir racours à un service d'inspection des installations électriques, ou à un électricien, selon le cas.

AVIS : L'indice d'équivalence de la sonnerie (IES) assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface. La terminaison d'une interface téléphonique peut consister en une combinaison de quelques dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Summary of System Commands

User Code Commands	Add A User Code = User Code + 8 + New User Number + New User's Code Change a Code = User Code + 8 + User Number + New User's Code Delete a User's Code = Your User Code + 8 + User Number to Be Deleted + Your Code Again View User Capability = User's Code + [✳] + [✳] Set Real-Time Clock (Installer, Master Only) = Code + [#] + 63	
Programming Commands	Site Initiated Download = User Code + [#] + 1. Activate Panel initiated Communication Session with Compass via the Dialer = Installer Code + [#] + 1. Direct-Wire Download Enable = User Code + [#] + 5. Enter Program Mode = Installer Code + 8000. Enter Interactive Program Mode = Installer Code + 8000 + [#] + 93 Exit Program Mode = ✳99 or ✳98.	
Event Logging Commands	Event Log Display = Code + [#] + 60 (Installer or Master Only) Event Log Print = Code + [#] + 61 (Installer or Master Only) Clear Event Log = Code + [#] + 62 (Installer or Master Only)	
Wireless System Commands	House ID Sniffer Mode = Code + [#] + 2 (Installer Only) Transmitter ID Test = Code + [#] + 3 (Installer Only) Go/No Go Test = Code + 5 (Test Key)	
Additional Commands	Partition GOTO	User Code + [✳] + Partition Number 0-8.
	GOTO Home Partition	User Code + [✳] + 0.
	Panics	[✳] + 1 or A Key (Zone 995). [✳] + [#] or B Key (Zone 999). [#] + 3 or C Key (Zone 996).
	View Downloaded Messages	Press 0 for 5 Seconds.
	Display All Zone Descriptors	Press [✳] for 5 Seconds.
Output Device Control Commands	Activate Output Device as Programmed = User Code + [#] + 71. Activate Output Device as Programmed = User Code + [#] + 72. Activate Output Device Manually = User Code + [#] + 70. Activate Output Device or System Event Instantly = User Code + [#] + 77. Randomize Output Devices = User Code + [#] + 41 Randomize Output Devices Programmed with Activation Times Between 6 PM and 5 AM = User Code + [#] + 42. De-activate Randomization = Enter the sequence used to activate randomization.	
Scheduling Commands	Installer-Programmed Schedule Events = Installer Code + [#] + 80 (Installer or Master Only). Temporary Schedule Editing = User Code + [#] + 81 (Installer, Master, Manager Only). Extend Closing Window = User Code + [#] + 82 (Installer, Master, Manager Only). End User Output Device Programming = User Code + [#] + 83.	

Access Control Commands	Activate Access Relay for Current Partition = User Code + 0. Request to Enter/Exit = User Code + [#] + 73. Request to Enter/Exit at Access Point = User Code + [#] + 74 + Access Point Number. Change Access Point State = User Code + [#] + 75 + Access Point + State. Perform a Test of the VistaKey Module = Installer Code + [#] + 78. Perform an Access Control Card Function = User Code + [#] + 79.
Master Code #65	If local programming lockout is set via downloading, programming mode cannot be entered at the keypad. In the event that local programming is required after the lock-out, setting the location in Compass will open a 24-hour window for programming when the Master code + #65-command is entered. The 24-hour window counts down and then locks out local programming until the next Master code + #65-command is entered.

Specifications

VISTA-128BPT/VISTA-250BPT CONTROL

Physical:

Standard Cabinet (included)	12 1/2" W x 14 1/2" H x 3" D
UL Cabinet (optional)	14 1/2" W x 18" H x 4.3" D (Included in the COM-UL Commercial Enclosure)

Electrical:

Voltage Input:	From ADEMCO No. 1361 Plug-In Transformer (use 1361CN in Canada) or 1361X10 transformer (for X-10 installations) rated 16.5VAC, 40 VA.
Alarm Sounder Output:	10VDC-13.8VDC, 1.7A max. (UL1023, UL609 installations); 750mA less aux. current draw (UL985 installations).
Auxiliary Power Output:	9.6VDC-13.8VDC, 750mA max. For UL installations, the accessories connected to the output must be UL Listed, and rated to operate in the above voltage range.
Backup Battery:	12VDC, 4AH or 7AH gel cell. YUASA NP4-12 (12V, 4AH) or NP7-12 (12V, 7AH) recommended.
Standby Time:	4 hours min. with 750 mA aux. load using 7 AH battery.
Circuit Protectors:	PTC circuit breakers are used on battery input to protect against reverse battery connections and on alarm sounder output to protect against wiring faults (shorts). A solid-state circuit breaker is used on auxiliary power output to protect against wiring faults (shorts).

Digital Communicator

Formats Supported:	4 + 2 Express, Contact ID and 10-Digit Contact ID
Line Seize:	Double Pole
Ringer Equivalence:	0.7B
FCC Registration No.:	AC398U-68192-AL-E

Remote Keypads

6160

Physical:

Width:	7.437 inches
Height:	5.25 inches
Depth:	1.312 inches

Electrical:

Voltage Input:	12VDC
Current Drain:	150mA

Interface Wiring:

RED:	12VDC input (+) auxiliary power
GREEN:	Data to control panel
YELLOW:	Data from control panel
BLACK:	Ground and (-) connection from supplemental power supply

6160V

Physical:

Width:	7 3/8 inches
Height:	5 5/16 inches
Depth:	1 3/16 inches

Electrical:

Voltage Input:	12VDC
Current Drain:	190mA

Interface Wiring:

RED:	12VDC input (+) auxiliary power
GREEN:	Data to control panel
YELLOW:	Data from control panel
BLACK:	Ground and (-) connection from supplemental power supply

APPENDIX D

Contact ID Codes

TABLE OF CONTACT ID CODES

Code	Definition
110	Fire Alarm
111	Smoke Alarm
121	Duress
122	Silent Panic
123	Audible Panic
124	Duress Access Grant
125	Duress Egress Grant
131	Perimeter Burglary
132	Interior Burglary
133	24-Hour Burglary
134	Entry/Exit Burglary
135	Day/Night Burglary
140	ACS Zone Alarm
150	24-Hour Auxiliary
162	CO Alarm
301	AC Loss
302	Low System Battery
305	System Reset
306	Program Tamper
308	System Shutdown
309	Battery Test Fail
313	System Engineer Reset
320	ACS Relay Supervision
321	Bell 1 Trouble
332	Poll Loop Short-Trouble
333	Expansion Module Failure
338	ACS Module Low Battery
339	ACS Module Reset
342	ACS Module AC Loss
343	ACS Module Self-Test Fail
344	RF Receiver Jam Detect
351	Telco Line 1 Fault
354	Communication Fail
373	Fire Loop Trouble
374	Exit Error by Zone
378	Cross Zone Trouble
380	Trouble (global)
381	Loss of Supervision (RF)
382	Loss of RPM Supervision
383	RPM Sensor Tamper
384	RF Transmitter Low Battery
385	Smoke Detector HI
386	Smoke Detector LO
389	Detector Self-Test Failed
401	O/C by User
403	Power-Up Armed/Auto-Arm
406	Cancel by User
407	Remote Arm/Disarm (Download)
408	Quick Arm
409	Keyswitch O/C
411	Callback Requested

Code	Definition
421	Access Denied
422	Access Granted
423	Door Force Open
424	Egress Denied
425	Egress Granted
426	Door Prop Open
427	Access Point DSM Trouble
428	Access Point RTE Trouble
429	ACS Program Entry
430	ACS Program Exit
431	ACS Threat Change
432	Access Point Relay/Trigger Fail
433	Access Point RTE Shunt
434	Access Point DSM Shunt/Unshunt
441	Armed STAY
451	Early Open/Close
452	Late Open/Close
453	Fail to Open
454	Fail to Close
455	Auto-Arm Fail
459	Recent Close
501	ACS Reader Disable
520	ACS Relay Disable
570	Bypass
576	ACS Zone Shunt
577	ACS Point Bypass
579	Vent Zone Bypass
602	Communicator Test
606	Listen-In to Follow
607	Burglary Walk-Test
621	Event Log Reset
625	Time/Date Reset
631	Exception Schedule Change
632	Access Schedule Change

NOTE: For Canadian controls, if there is a phone line (or radio) failure and the panel has exhausted its maximum attempts to send reporting events to the central station, the panel will hold the messages in a buffer and resend upon restoral of the communication path. In addition, old messages that are sent will indicate that they are not current messages so that the central station does not dispatch on them. In order to accomplish this, an event qualifier of "6" will be sent in place of the "1" or "3" character in the message. The "6" indicates that the message is old. Events will be sent in chronological order and will be time-stamped in the system's event log.

Event Log Alpha Descriptors

Alpha	Event Description
FIRE	Fire Alarm
DURESS	Duress Alarm
PANIC	Silent or Audible Panic Alarm
BURGLARY	Burglary Alarm
EXP SHRT	Polling Loop Short
RF EXPND	Expander Module Failure
AUXILIARY	Non-burglary Alarm
TROUBLE	Trouble

Alpha	Event Description
AC LOSS	AC Loss
LOW BATTERY	System Low Battery
SYSTEM RESET	System Reset
PROG CHANGE	Program Change
BATTERY FAIL	System Battery Failure
RF SUPR	RF Supervision
RPM SUPR	RPM Supervision
RF LBAT	RF Low Battery

Alpha	Event Description
EXP TRBL	Expander Module Trouble
RF TRBL	RF Trouble
TAMPER	Tamper
FIRE TRB	Fire Trouble
FAIL TO COMM	Failure to Communicate
BELL TROUBLE	Bell Trouble
DISARMED	Disarmed
DISARMED-REM	Disarmed Remotely
DISARMED-KEY	Disarmed Via RF Key
DISARM-AUTO	Auto-Disarm
CALL BACK	Callback Requested
CANCEL	Cancel
DISRMD-EARLY	Disarmed Early
DISRMD-LATE	Disarmed Late
MISSED DISRM	Missed Disarm
SKED CHANGE	Schedule Change
ACC SKED CHG	Access Control Schedule Change
ARM FAILED	Failed to Arm
DIALER SHUT	Dialer Shutdown
SYSTEM SHUT	System Shutdown
BYPASS	Bypass
SELF TEST	Self-test
TEST ENTRY	Manual Test Entry
TEST EXIT	Manual Test Exit
LOG OVERFLOW	Dialer Queue Overflow
LOG CLEARED	Event Log Cleared
TIME SET	Time Set
TIME ERROR	Time Error
PROGRM ENTRY	Program Entry
PROGRAM EXIT	Program Exit
Uxxx ADD BY	User XXX Added BY
Uxxx DEL BY	User XXX Deleted BY
Uxxx CHG BY	User XXX Changed BY
PRINTER FAIL	Event Log Printer Failure
TESTED	Zone Tested
UNTESTED	Zone Untested
FAILED	Zone Test Failed
RLY TRBL	Relay Trouble
EXP TMPR	Expansion Module Tamper
VENT BYPASS	Vent Zone Bypass
RF JAM	RF Jam Detected
JAM RSTR	RF Jam Restore
FIRE RST	Fire Alarm Restore
DURE RST	Duress Alarm Restore
PNC RST	Panic Alarm Restore
BURG RST	Burglary Alarm Restore
EXP RST	Expansion Module Restore
RF RST	RF Restore
AUX RST	Auxiliary Restore
MED RST	Medical Restore
TRBL RST	Trouble Restore
AC RESTORE	AC Restore
LOW BATT RST	System Low Battery Restore
PROG CHANGE	Program Change
BAT TST FAIL	Battery Test Failure
RPM RST	V-Plex Restore
RFLB RST	RF Low Battery Restore
EXP RST	Expansion Module Failure Restore
TMPR RST	Tamper Restore
FRTR RST	Fire Trouble Restore
COMM RESTORE	Communication Restore
RLY RST	ECP Relay Trouble Restore
ARMED	Armed
ARMED-STAY	Armed Stay
ARMED-REM	Armed Remotely
ARMED-QUICK	Quick Armed
ARMED-KEY	Armed Via RF Key
ARMED-AUTO	Auto-Armed
PARTIAL ARM	Partial Armed

Alpha	Event Description
ARMED-EARLY	Armed Early
ARMED-LATE	Armed Late
MISSED ARM	Missed Arm
DIALER RST	Dialer Restore (Shutdown)
SYSTEM RST	System Restore (Shutdown)
BYP RST	Bypass Restore
TEST EXIT	Test Mode Exit
PRINTER RSTR	Printer Restore
BELL RESTORE	Bell Restore
EXIT ERR	Exit Error
RECENT ARM	Recent Arm
VENT BYP RST	Vent Zone Bypass Restore
DIALER FULL	Dialer Overflow
Access Control Events	
ACS PNT	Access Point Failure
DSM SHNT	Door Status Monitor Shunt
DUR ACCS	Duress Access Grant
NO ENTRY	Access Denied
DR OPEN	Door Propped Open
DR FORCE	Door Forced Open
ENTERED	Access Granted
NO EXIT	Egress Denied
ACPT BYP	Access Point Bypass
RTE SHNT	Request to Exit Shunt
EXITED	Egress Granted
ACLO MOD	AC Loss at Module
LBAT MOD	Low Battery at Module
COMM MOD	Comm Failure from MLB to Module
RES MOD	Access Control Module Reset
ACPT RLY	Access Point Relay Supervision Fail
SELF MOD	Module Self-Test Failure
ACZN CHG	Access Control Zone Change
ACS PROG	Access Control Program Entry
ACS PRGX	Access Control Program Exit
THRT CHG	Access Control Threat Change
SYS SHUT	System Shutdown
SYS RST	System Engineer Reset
ZN SHUNT	Access Control Zone Shunt
ZN ALARM	Access Control Zone Alarm
RDR DISA	Access Control Reader Disable
RLY DISA	Access Control Relay/Trigger Disable
RTE TRBL	Request to Exit Point Trouble
DSM TRBL	Door Status Monitor Point Trouble
DUR EXIT	Duress Egress Grant
BGN ACS TEST	Access Control Test Mode Start
ACPT RST	Access Point Restore
ACRST MOD	AC Loss at Module Restore
LBAT RST	Low Battery at Module Restore
COMM RST	Comm Fail MLB to Module Restore
RLY RST	Access Point Relay Supervision Rest
SELF RST	Self-Test at Module Restore
ACPT UNB	Access Point Unbypass
DSM UNSH	Door Status Monitor Unshunt
RTE UNSH	Request to Exit Point Unshunt
DRFO RST	Door Forced Open Restore
DRPO RST	Door Propped Open Restore
DSM RST	Door Status Monitor Trouble Restore
RTE RST	Request to Exit Point Trouble Rest
RLY ENAB	Access Control Relay/Trigger Enable
RDR ENAB	Access Control Reader Enable
ZNAL RST	Access Control Zone Restore
ZN UNSHT	Access Control Zone Unshunt
SYSHTRST	System Shutdown Restore
END ACS TEST	Access Control Test Mode End

Index

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

W

X

Y

Z

WARNING!
THE LIMITATIONS OF THIS ALARM SYSTEM

While this System is an advanced wireless security system, it does not offer guaranteed protection against burglary, fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

- Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
- Intrusion detectors (e.g., passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Battery-operated devices will not work without batteries, with dead batteries, or if the batteries are not put in properly. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.
- Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
- A user may not be able to reach a panic or emergency button quickly enough.
- While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second floor detector, for example, may not sense a first floor or basement fire. Finally, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson. Depending on the nature of the fire and/or location of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.
- Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of the protected area approaches the temperature range of 90° to 105°F (32° to 40°C), the detection performance can decrease.
- Alarm warning devices such as sirens, bells or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices are located on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled by noise from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm-warning devices, however loud, may not warn hearing-impaired people.
- Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily out of service. Telephone lines are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.
- This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 20 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly. The security keypad (and remote keypad) should be tested as well.

Wireless transmitters (used in some systems) are designed to provide long battery life under normal operating conditions. Longevity of batteries may be as much as 4 to 7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, high or low temperatures, as well as large swings in temperature, may all reduce the actual battery life in a given installation. This wireless system, however, can identify a true low battery situation, thus allowing time to arrange a change of battery to maintain protection for that given point within the system.

Installing an alarm system may make the owner eligible for a lower insurance rate, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property. We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

For the latest warranty information, please go to:
www.honeywell.com/security/hsc/resources/wa

Notes

Notes

Notes

Honeywell

2 Corporate Center Drive, Suite 100
P.O. Box 9040, Melville, NY 11747

www.honeywell.com/security

800-06903 6/10 Rev A