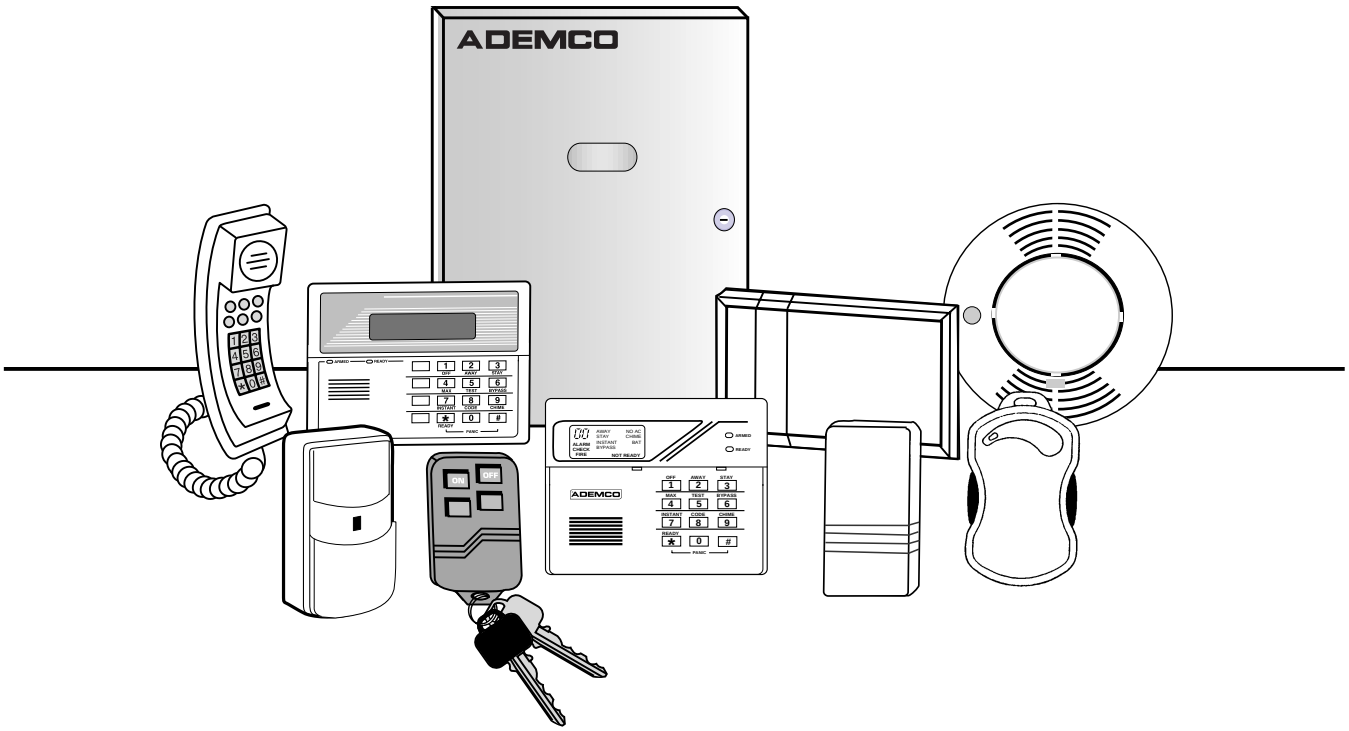
# VISTA-128B

## Commercial Burglary

## Partitioned Security System

## with Scheduling

## Installation and Setup Guide




®ADEMCO

.

K3271V1 9/00

.

# 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 which 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 which, 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.

| Enter Zn Num.<br>00 = Quit |
|---|

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 When programming the system, data fields are indicated by a "star" (✳) followed by the data field number.

**PRODUCT MODEL NUMBERS:** Unless noted otherwise, references to specific model numbers represent ADEMCO products.

# General Description

***In This Section***



## General

The VISTA-128B is an 8-partition, UL commercial burglary control panel that supports up to 128 zones using basic hardwired, polling loop, and wireless zones. It also includes zones for supervision of bells, phone lines, keypads, RF Receivers, and relays. In addition, the control offers scheduling capabilities and allows certain operations to be automated by pressing a single button. The system has the capability to interface with an ECP long range radio unit that can send Contact ID messages and an alpha numeric paging device. The control can be connected to the ADEMCO PassPoint system (via the Vista Gateway Module) or a VistaKey module (via the polling loop) to provide a fully integrated security and access control system.

## Features

### Basic Hardwired Zones

Provides 9 style-B hardwire zones with the following characteristics:

- EOLR supervision (optional for zones 2-8) supporting N.O. or N.C. sensors

  (EOLR supervision required for fire and UL burglary installations)
- Individually assignable to one of 8 partitions
- Up to 16 2-wire smoke detectors on zone 1
- 4-wire smoke or heat detectors on zones 1-8 (power to 4-wire smoke detectors must be supervised with an EOL device)
- Up to 50 2-wire latching glassbreak detectors on zone 8

### Optional Expansion Zones

#### Polling Loop Expansion

Supports up to 120 additional hardwire zones using a built-in polling (multiplex) loop interface. Current draw can total up to 128mA. Polling loop zones have the following characteristics:

- Must use RPM (Remote Point Module) devices
- Supervised by control panel
- Individually assignable to one of 8 partitions

### Wireless Expansion

Supports up to 128 wireless zones using 5881 type RF receiver (fewer if using hardwire and/or polling loop zones). Wireless zones have the following characteristics:

- Supervised by control panel for check-in signals (except certain nonsupervised transmitters)
- Tamper protection for supervised transmitters
- Individually assignable to one of 8 partitions

---

**UL** Wireless devices may not be used in UL commercial burglary installations.

---

For specific information regarding number of wireless zones supported, see the section *Wireless Zone Expansion* later in this manual.

---

### System Zones

Provides zones for supervision of all peripheral devices (keypads, RF receivers, and relay modules) and individual relays, as well as system zones (RF receivers and keypad panics). Zone assignments are as follows:

| | |
|---|---|
| Individual Relay Zones | 601-632 |
| Peripheral Device Zones | 800-831 |
| System Zones | 988-999 |

(See the *Zone Index/Zone Type Defaults* section for a full explanation of these zones and specific zone assignments.)

### 8 Partitions

Provides the ability to control 8 separate areas independently, each functioning as if it had its own separate control. Partitioning features include:

- A Common Lobby partition (1-8), which can be programmed to arm automatically when the last partition that shares the common lobby is armed and to disarm when the first partition that shares the common lobby is disarmed
- A Master partition (9), used strictly to assign keypads for the purpose of viewing the status of all 8 partitions at the same time (master keypads)
- All zones assignable to one of 8 partitions
- Keypads assignable to one of 8 partitions or to Master partition 9 to view system status
- Ability to assign relays to one or all 8 partitions
- Ability to display fire and/or burglary and panic and/or trouble conditions at all other partitions' keypads (selectable option)
- Certain system options selectable for each partition, such as entry/exit delay and subscriber account number

### User Codes

Accommodates 150 user codes, all of which can operate any or all partitions. Certain characteristics must be assigned to each user code, which are as follows:

- Authority level (Master, Manager, or several other Operator levels)
- Opening/Closing central station reporting option
- What partitions the code can operate
- Global arming capability (ability to arm all partitions the code has access to in one command)
- Use of an RF (button) to arm and disarm the system (RF key must first be enrolled into the system)

### Peripheral Devices

Supports up to 31 addressable devices, which can be any combination of keypads (6139), RF receivers (5881), relay modules (4204/4204CF), and 4285/4286 VIP module. Peripheral devices have the following characteristics:

- Each device set to an individual address (physically) according to the device's instructions
- Each device enabled in the system using *Device Programming* (covered later in this manual)

At least one 2-line alpha keypad (6139) must be connected to the system for programming (if 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.

### Keypad Panic Keys

Accommodates three keypad panic keys: 1 + ✳ (A), ✳ + # (B), and 3 + # (C).

- Designated as zones 995 (1 + ✳), 996 (3 + #), and 999 (✳ + #)
- Activated by wired and wireless keypads
- Activated and reported separately by partition, distinguished by subscriber account number (or partition number if Contact ID reporting is used)

### Keypad Macros

Accommodates 32 keypad macro commands per system (each macro is a series of keypad commands). For example, by pressing either the A, B, C, or D key, the system can be programmed to log onto another partition, bypass Zones 2 and 3, and arm that partition in the AWAY mode (explained in detail later in this manual). Characteristics of keypad macros are:

- Assignable to the A, B, and C keys by partition
- Other macros, (not assigned to these keys) executed by using the D key
- Each macro can be 32 characters (keystrokes) in length

### Optional Output Devices

Accommodates the use of 96 outputs using ADEMCO's 4204 and 4204CF Relay Modules, Fire System Annunciators (FSA-8, FSA-24), V-Plex Relay Modules and Powerline Carrier Devices (X-10). Each 4204 module provides four Form C relays for general purpose use. Each 4204CF provides two style-Y supervised bell outputs. The FSA-8 provides 8 LED outputs and the FSA-24 provides 24 LED outputs.

The outputs have the following characteristics:

- Can be programmed to activate in response to system events
- Can be programmed to activate using time intervals
- Can be used for style-Y supervised bell outputs (4204CF only)
- Can be activated manually using the #70 Relay Command Mode
- Can be activated instantly using the #77 Command Mode
- Can be supervised by control panel (zones 601-632)
- 1-32 can have an alpha descriptor assigned to it

### Optional Vista Interactive Phone Module

Supports the ADEMCO 4285/4286 VIP Module. This permits access to the security system to do the following:

- Obtain system status information
- Arm and disarm security system
- Control relays

---

**UL** The 4285/4286 VIP Module is not Listed for use with the VISTA-128B Control Panel in a UL commercial installation.

---

### Access Control

If programmed, provides users with a command that activates relays to open access doors (e.g., lobby door). Each partition can be assigned to an access control relay.

By using one Vista Gateway Module (VGM), the control can be connected to the ADEMCO PassPoint system for a fully integrated access control system.

The VistaKey module may also be used for access control. It is a single-door access control module that, when connected to the VISTA-128B, provides access control to the protected premises. The system can support up to 8 VistaKey modules (8 access points) and up to 250 access cards.

---

**UL** The access control function is not Listed for use with the VISTA-128B Control Panel in a UL commercial installation.

---

### Optional Keyswitch

Supports the ADEMCO 4146 Keyswitch on any one of the system's 8 partitions. If used, zone 7 is no longer available as a protection zone.

### Voltage Triggers

Provides a trigger connector whose pins change state for different conditions. Used with LRR (Long Range Radio) equipment or other devices such as a remote keypad sounder, keyswitch ARMED and READY LEDs, or a printer to print the system's event log.

### Event Log

Keeps a log of different event types (enabled in programming). The event log has the following characteristics:

- Stores up to 512 events
- Can be viewed at the keypad or through the use of Compass software
- Can be printed on a serial printer using a 4100SM Module including zone alpha descriptors
- Can store PassPoint events
- Printed events can be sent to an alpha numeric pager

### Scheduling

Provides the following scheduling capabilities:

- Open/close schedules (for control of arming/disarming and reporting)
- Holiday schedules (allows different time windows for open/close schedules)
- Timed events (for activation of relays, auto-bypassing and unbypassing, auto-arming and disarming, etc.)
- Access schedules (for limiting system access to users by time)
- End User Output Programming Mode (provides 20 timers for relay control)

### Communication Formats

Supports the following formats for the primary and secondary central station receivers:

- ADEMCO Low Speed (Standard or Expanded)
- Sescoa/Radionics
- ADEMCO Express
- ADEMCO High Speed
- ADEMCO Contact ID
- Long Range Radio interface (ECP)

### Audio Alarm Verification Option

Provides a programmable Audio Alarm Verification (AAV) option which can be used in conjunction with an output relay to permit voice dialog between an operator at the central station and a person at the premises. An optional AAV unit, such as Eagle model 1250, is required.

---

**UL** The Eagle Model 1250 AAV unit is not UL Listed.

---

### Cross-Zoning Capability

Helps prevent false alarms by preventing a zone from going into alarm unless its cross-zone is also faulted within 5 minutes.

### Exit Error False Alarm Prevention Feature

- System can tell the difference between a regular alarm and an alarm caused by leaving an entry/exit door open. If not subsequently disarmed, faulted E/E zone(s) and/or interior zones will be bypassed and the system will arm.
- Generates an Exit Error report by user and by zone to the central station.

### Built-in User's Manual and Descriptor Review

For end-user convenience, the VISTA-128B contains a built-in User's Manual. By depressing any of the function keys on the keypad for 5 seconds, a brief explanation of that function scrolls across the alpha-numeric display. In addition, all programmed zone descriptors can be displayed (one at a time) by pressing the READY key for 5 seconds. This serves as a check for installers to be sure all descriptors are entered properly.

### Improved Downloading Features

- Uploads and downloads at 300 baud, making upload/download speed faster.
- Ability to upload ECP devices, their physical addresses, programmed addresses, and firmware revision levels from the control.

### Agency Listings

#### Burglary

- UL609 Grade A Local Mercantile Premises and Mercantile Safe and Vault
- UL611/UL1610 Grades A, AA Central Station
- UL365 Grades A, AA Police Connect

# Planning a Partitioned System

### In This Section



## Theory of Partitioning

This system provides the ability to arm and disarm up to 8 different areas, as if each had its own control. These areas are called partitions. Partitions are used 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 prescribed options, see *The Mechanics of Programming*, section as well as each corresponding section's programming procedure.

To setup a partitioned system perform the following steps:

| Step | Action |
|---|---|
| 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).

This option employs logic for automatic arming and disarming of the common lobby. Two programming fields affect 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 option to 1 for a specific partition causes that partition to affect the operation of the common lobby as follows:

- When the first partition that affects the lobby is disarmed, the lobby will also be disarmed.
- The common lobby cannot be armed unless every partition selected to affect the lobby is armed.
- Arming the last partition that affects the lobby will not cause the system to automatically attempt to arm the lobby.

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

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

- When the first partition that affects the lobby is disarmed, the lobby will also be disarmed.
- The common lobby cannot be armed unless every partition selected to affect the lobby is armed.
- Arming the last partition that is programmed to arm the lobby will cause the system to automatically attempt to arm the lobby. If any faults exist in the lobby partition, or another partition that affects the lobby is disarmed, the lobby cannot be armed, and the message "UNABLE TO ARM LOBBY PARTITION" will be displayed.

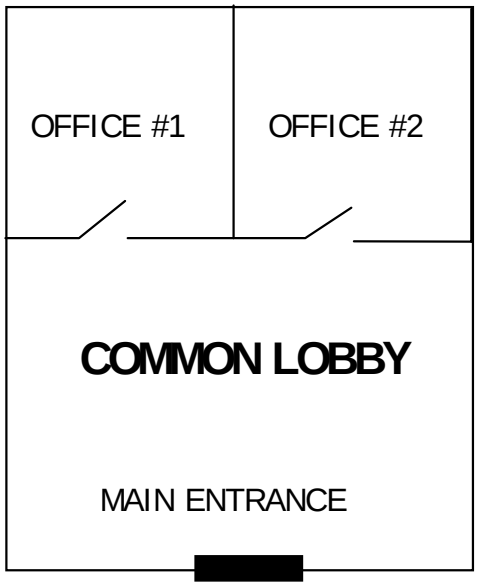
You cannot select a partition to "arm" the lobby unless it has first been selected to "affect" the lobby. Enable field 1*18 before enabling field 1*19.

The following chart sums up how the common lobby partition will operate, if different options are set for another partition in fields 1*18 and 1*19.

| 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.

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, since 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 the *User Access Codes* section), the keypad will ask "Arm all?" or "Disarm all?" whenever the user tries to arm or disarm the partitions he has access to from an alpha keypad. 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 attempting to arm all, and another "affecting" partition is disarmed, the user will not be able to arm the lobby, and the message "UNABLE TO ARM LOBBY PARTITION" will be displayed.

*Codes with Non-Global Arming*

If arming with a non-global code, the lobby partition operation will be automatic, as described by fields 1*18 and 1*19.

### Other Methods of Arming/Disarming

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 arming or disarming remotely (through Compass downloading software), the lobby will 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 will 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 using auto-arming, make sure that the **Auto-Arm Delay** and **Auto-Arm Warning** periods (fields 2*05 and 2*06) combined are longer than that of any other partition that affects the lobby. This will cause 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.

Any keypad assigned to Partition 9 in *Device Programming* in the *#93 Menu Mode* will make 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 ✳B
```

Possible status indications include:

| | |
|---|---|
| A = Armed Away | M = Armed Maximum |
| S = Armed Stay | I = Armed Instant |
| R = Ready | N = Not Ready |
| B = Bypassed/Ready | ✳ = Alarm Memory/Trouble present |

To obtain more information regarding a particular partition, enter ✳ + [Partition No.] (i.e., ✳4). This will allow 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 will be denied.

The following would be displayed for a fault condition on Zone 2 (Loading Dock Window) on Partition 1 (Warehouse) when logging on from a keypad on Partition 9:

```
WHSE DISARMED
HIT ✳ FOR FAULTS
```

Pressing ✳ will cause the following display to appear at Partition 1's keypad(s):

```
FAULT 002  LOADING
DOCK WINDOW
```

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

The Armed LED on a master keypad will be lit only if all partitions have been armed successfully. The Ready LED will be lit only if all partitions are "ready to arm." Neither LED will be lit if only some partitions are armed and/or only some partitions are ready.

The sounder on a master keypad will reflect the sound of the most critical condition on all of the partitions. The priority of the sounds is as follows:

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

# False Alarm Reduction Features

### In This Section



## General Information

This control supports features that help minimize false alarms. Most false alarms occur upon exiting the premises, either due to environmental factors, or because the zone's resistance to the control may be on the edge of acceptability. We call this condition a "swinger."

Features which prevent false alarms due to these circumstances are:

- Exit Error Logic and related reports
- Exit Delay Reset
- Cross-Zoning

## Exit Error Logic and Related Reports

**UL** This feature is not suitable for use on a UL commercial burglary installation.

This feature is intended to reduce the incidence of false alarms due to exit doors that are left open after the exit delay has expired. If this feature is enabled in program field 1*20, the following will occur:

At the end of the exit delay, if a door is left open or an interior zone is faulted, the system will start the entry delay period, and will sound 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 will bypass the faulted entry/exit and/or interior zone(s). The rest of the system will be armed. In addition, the following dialer reports will be sent to the central station if programmed:

- Exit Error by User (not sent if using ADEMCO High Speed format)
- Exit Error by Zone (Sent as regular alarm if using ADEMCO High Speed format)
- Bypass reports

## Recent Close Report

Another report, designed to notify the central station that an alarm has occurred within 5 minutes of arming, is called the **Recent Close** report. This report, as well as the Exit Error reports, are programmed in *Report Code Programming* in the *#93 Menu Mode*.

## Exit Delay Reset

**UL** This feature is not suitable for use on a UL commercial burglary installation.

This feature is designed to allow an operator to re-enter the premises to retrieve a forgotten item without triggering an alarm. This feature is enabled in program field 1*21, and works in the following way:

When the panel is armed, the normal exit delay begins. After the user exits and the door closes, the exit delay time is reset to 60 seconds. If, within this 60-second period, the entry door is re-opened, the panel will restart the exit delay sequence using the programmed exit delay time. This feature will only be activated once after arming.

## Cross Zoning

**UL** This feature is not suitable for use on a UL commercial burglary installation.

The Cross-Zoning feature is designed so that a combination of two zones must be faulted within a 5 minute period of each other to cause an alarm on either zone. This prevents momentary faults from one of the zones causing an alarm condition. You can select four "sets" of cross-zones, keeping in mind the following:

- Both must protect the same area.
- Both must be in the same partition.
- A fire zone must only be crossed to another fire zone protecting the same physical area **(see warning below).**

**Note:** The four sets of cross-zones are programmed in data fields 1*22, 1*23, 1*24, and 1*25.

DO NOT cross-zone a fire zone with a burglary zone under any circumstance. A fire zone must only be crossed to another fire zone and BOTH must be protecting the same physical area (no walls or partitions separating them). Consult NFPA 72 standard for exact spacing requirements. As a guideline, we recommend that spacing between fire cross-zones be no farther than 30 ft.

### Conditions That Affect Cross-Zone Operation

- In the event of a continuous fault (lasting at least 5 minutes) on one of the paired zones, a fault on the second zone will cause an alarm immediately.
- If one of the zones in a pair is bypassed or has a zone response type set to 0, the cross-zoning feature will 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 will ensure 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 will activate 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).

## Call Waiting Defeat Logic

Although this option does not directly prevent false alarms, it may prevent the central station from taking action on a potential false alarm. 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) would hear the phone ringing indefinitely and have to dispatch on the call.

This option, enabled in program field 1*42, attempts to defeat Call Waiting on the first outgoing call attempt to both the primary and secondary numbers. It does this by dialing a special sequence preceding the phone number (but after the PABX number). The panel will dial *70 if using TouchTone and 1170 if using rotary.

The panel does not attempt to defeat Call Waiting on each call attempt, because the phone company may not complete the call if the sequence is dialed on a phone line that does not have Call Waiting.

# Installing The Control

### In This Section



## Mounting the Control Cabinet

- Mount the control cabinet to a sturdy wall using fasteners or anchors (not supplied) in a clean, dry area which is not readily accessible to the general public. The back of the control cabinet has 4 holes for this purpose.
- 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.

## Installing the Cabinet Lock

Use an ADEMCO No. N6277 Cam Lock and No. P3422-2 Clip for universal commercial cabinet.

To install the cabinet lock, perform the following steps:

| Step | Action |
|---|---|
| 1 | Insert the key into the lock. Position the lock in the hole making certain that the latch will make contact with the latch bracket when the door is closed. |
| 2 | While holding the lock steady, insert the retainer clip into the retainer slots. |

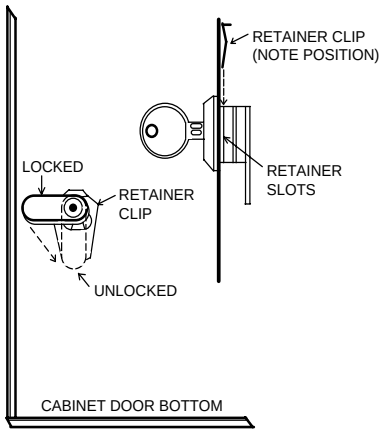



***Figure 4-1: Installing the Lock***

**UL** To provide certificated burglary service for UL installations, refer to the special requirements and *Figure 4-2 Cabinet Attack Resistance Considerations* to follow.

## Grade A Mercantile Premises Listing

For a Grade A Mercantile Premises listing, perform the following steps:

| Step | Action |
|---|---|
| 1 | **The panel door must be supervised.** Mount the clip-on tamper switch (supplied) to the cabinet's right side wall as shown in *figure 4-2*. Wire it to one of the hardwire zones. |
| 2 | **Use a bell with a tamper-protected housing** such as the ADEMCO AB12. The bell housing's tamper switch and inner tamper linings must also be wired to the hardwire zone. |
| 3 | **Assign the 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. |
| 4 | **All wiring between the bell and panel must be run in conduit.** Remaining wires do not need to be run in conduit. |
| 5 | **All wiring which is not run in conduit must exit from the knockout openings on the bottom or back of the cabinet.** |
| 6 | **All unused knockouts must be plugged** using the disc plugs and carriage bolts (supplied), as indicated in *figure 4-2*. |
| 7 | Fasten the cabinet door to the cabinet backbox using the 18 one-inch-long Philips-head screws (supplied) after all wiring, programming and checkout procedures have been completed. |

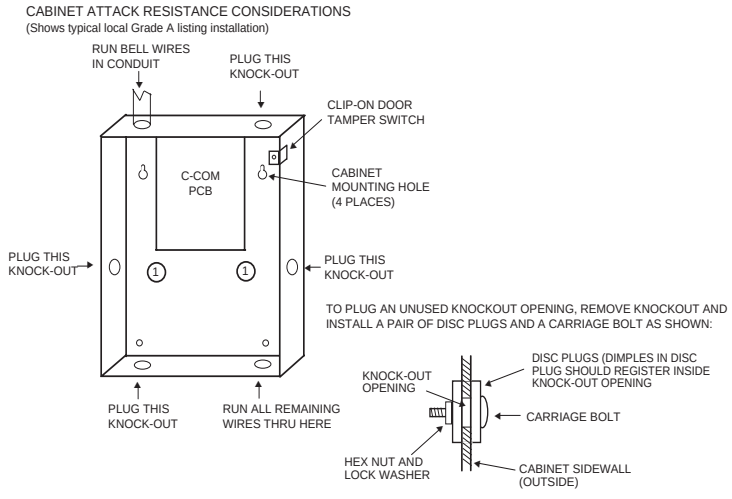



***Figure 4-2: Cabinet Attack Resistance Considerations***

## Grade A Mercantile Safe and Vault Listing

For a Grade A Mercantile Safe and Vault listing, perform the following steps:

| Step | Action |
|---|---|
| 1 | Follow the instructions given above for Mercantile Premises listing. |
| 2 | 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. |
| 3 | 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 control's circuit board, perform the following steps:

| Step | Action |
|---|---|
| 1 | Hang the three mounting clips on the raised cabinet tabs. Make sure the clip orientation is exactly as shown in *figure 4-3* to avoid damage to the clip when mounting screws are tightened. 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. |
| 3 | Swing the base of the board into the mounting clips and secure the board to the cabinet with the accompanying screws. |

Make certain that the mounting screws are tight. This ensures that there is a good ground connection between the PC board and the cabinet. Also, dress field wiring away from the microprocessor (center) section of the PC board. Use the 2 loops on the left and right sidewalls of the cabinet for anchoring field wiring using tie wraps. These steps are important to minimize the risk of panel RF interference with television reception.

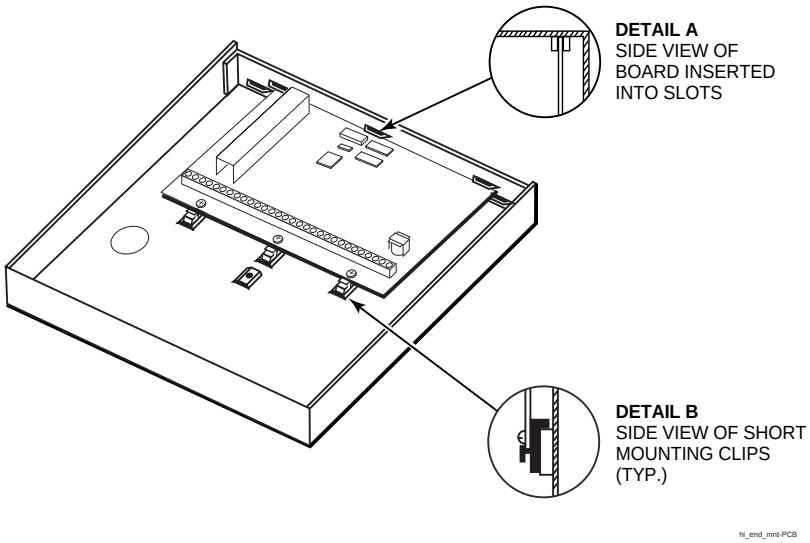



***Figure 4-3: Mounting the PC Board***

## AC Transformer and Battery

This product uses the 1361 transformer (1361CN in Canada). We recommend wiring all zones and expansion modules according to each section's instructions *before* powering up the system for programming and testing. Refer to the *Final Power-Up Procedure* section for specific instructions on how to connect the transformer and backup battery.

If using Powerline Carrier devices, the 4300 transformer interface must be used ***instead*** of the regular 1361 transformer. The 4300 supplies the control panel with AC, and also sends control pulses through the premises electrical system to control the Powerline Carrier devices. Refer to the *Final Power Up Procedure* for specific instructions on how to connect the 4300 transformer.

Refer to the *Final Power-Up Procedure* section for battery standby calculations and battery selection table.

## 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 further than 30 feet. The following are examples of good earth grounds available at most installations:

- **Metal Cold Water Pipe:** Use a non-corrosive 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 this connection in order for its lightning transient protection devices.

# Installing The Keypads

### In This Section



## Keypads That May Be Used

- ADEMCO 2-line alpha display keypads.
- Up to 16 addressable keypads may be used in the system, independent of auxiliary power considerations (you may need to use an auxiliary power supply if the 750mA aux. output is exceeded)

## Wiring to the Keypads

- The length of all wire runs combined must not exceed 2000 feet when unshielded quad conductor cable is used (1000 feet if unshielded cable is run in conduit or if shielded cable is used).
- If more than one keypad is wired to a 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).

To wire the keypads to the control, perform the following steps:

| Step | Action |
|---|---|
| 1 | Determine wire gauge by referring to the following wiring length/gauge table:<br>**Wire Run Length Table**<br>Wire Gauge: #22 gauge — Length: 450 feet<br>Wire Gauge: #20 gauge — Length: 700 feet<br>Wire Gauge: #18 gauge — Length: 1100 feet<br>Wire Gauge: #16 gauge — Length: 1750 feet |
| 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, & 9 on the control board, as shown in *Figure 5-1.* |

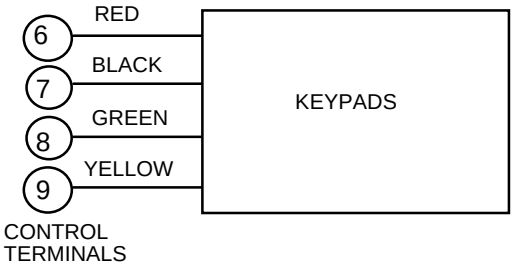



***Figure 5-1: Keypad Connections to Control Panel.***

## Using a Supplementary Power Supply to Power Additional Keypads

The control provides 750mA auxiliary standby power for powering keypads and other devices from the auxiliary power output. 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., Alarm-Saf Model AS/PS5-BFS-12-UL). Use a UL Listed, battery-backed supply for UL installations.

Connect the additional keypads as shown in *Figure 5-2*, using the keypad wire colors shown. Be sure to observe the current ratings for the power supply used.

1. Make connections directly to the screw terminals as shown in *Figure 5-2*. Make no connection to the keypad blue wire (if present).
2. Be sure to connect the negative (–) terminal on the power supply unit to terminal 7 (AUX **–**) on the control.

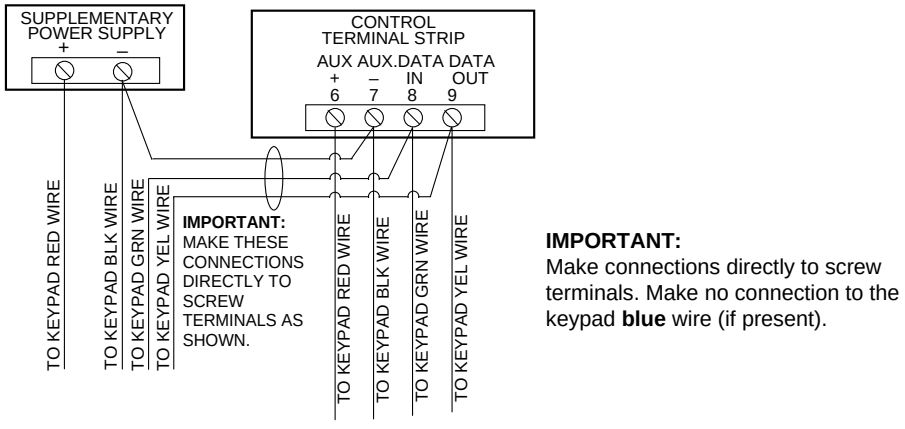



***Figure 5-2: Using A Supplementary Power Supply For Keypads***

## Mounting the Keypads

Mount the keypads at a height that is convenient for the user. Refer to the instructions provided with the keypad for mounting procedure.

You can either surface-mount or flush-mount keypads (using the 6139TRK Trim Ring Kit). Refer to the mounting instructions and template included with the keypad and/or trim ring kit for specific information.

## 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*.
- Each keypad must be assigned a different address.

To address the keypads, perform the following steps:

| Step | Action |
|---|---|
| | Power up the system temporarily. Use a fully charged 12VDC battery. |
| 2 | Set each keypad to an individual address (00-30) according to the keypad's instructions. Set one keypad for address 00 and other keypads for higher addresses (01 is enabled in the system's default program).<br>**Note:** Any keypads set for address 02 and above will appear blank until they are enabled in the system's program. |

Keypads set to the Nonaddressable Mode (address 31) will interfere with other keypads (as well as other devices) connected to the keypad terminals.

If an “OPEN CIRCUIT” message is present on the keypad, data from the control is not reaching the keypad. Please check your wiring.

# Basic Hardwired Zones 001-009

### In This Section



## Common Characteristics of Hardwired Zones 1-9

- EOLR supervision (optional for zones 2-8) supporting N.O. or N.C. sensors (EOLR supervision required for fire and UL Burglary installations)
- Individually assignable to one of 8 partitions
- Up to 16 2-wire smoke detectors on zone 1
- 4-wire smoke or heat detectors on zones 1-8 (power to 4-wire smoke detectors must be supervised with an EOL device)
- Up to 50 2-wire latching glassbreak detectors on zone 8

## Wiring Burglary and Panic Devices to Zones 1-9

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

| Step | Action |
|---|---|
| | Connect sensors/contacts to the hardwire zone terminals (10 through 23). See *Figure 6-1*. |
| 2 | Connect sensors/contacts to the hardwire zone terminals (10 through 23). |
| 3 | Connect N.O. devices **in parallel (across)** the loop. The 2K EOL resistor must be connected across the loop wires at the last device. |

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

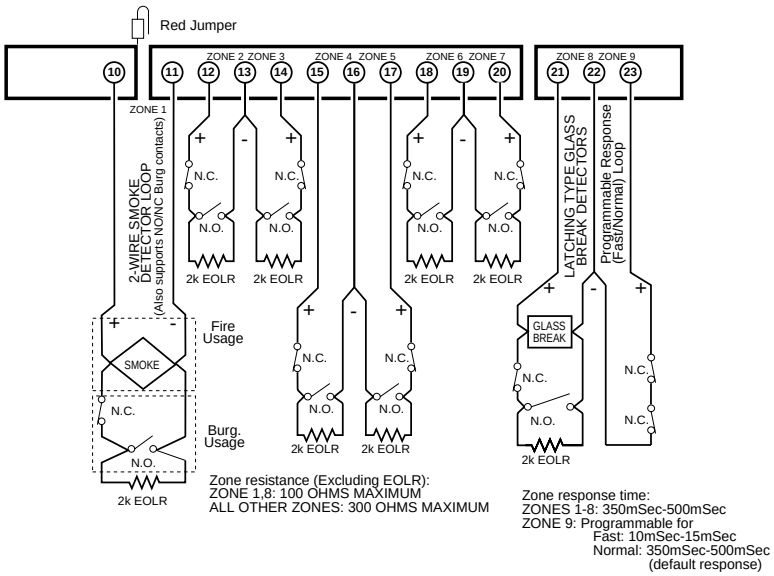



***Figure 6-1: Wiring Connections for Zones 1-9***

## Installing 2-Wire Smoke Detectors to Zone 1

Zone 1 has the added capability of supporting 2-wire smoke detectors. The zone provides enough standby current (2mA) to power up to 16 of the smoke detectors listed below. When assigned zone type 9, the second entry of a User Code + OFF sequence at a keypad will interrupt power to these zones to allow detectors to be reset following an alarm.

### Compatible 2-Wire Smoke Detectors

You may use up to 16 2-wire smoke detectors on zone 1 listed in the table below.

| DETECTOR TYPE | DEVICE MODEL # | DETECTOR TYPE | DEVICE MODEL # |
|---|---|---|---|
| Photoelectric, direct wire | System Sensor 2400 | Photoelectric duct detect. w/DH400 base | System Sensor 2451 |
| Photoelectric w/heat sensor, direct wire | System Sensor 2400TH | Ionization duct detector w/DH400 base | System Sensor 1451DH |
| Photoelectric w/B401B base | System Sensor 2451 | Ionization, direct wire | System Sensor 1100 |
| Photoelectric w/heat sensor and B401B base | System Sensor 2451TH | Ionization w/B110LP base | System Sensor 1151 |
| Ionization, direct wire | System Sensor 1400 | Photoelectric, direct wire | System Sensor 2100 |
| Ionization w/B401B base | System Sensor 1451 | Photoelectric w/heat sensor, direct wire | System Sensor 2100T |
| Photoelectric duct detect. w/DH400 base | System Sensor 2451 | Photoelectric w/B110LP base | System Sensor 2151 |

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

### Wiring 2-wire Smoke Detectors

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

| Step | Action |
|---|---|
| | Select from the list compatible 2-wire smoke detectors (up to 16). |
| 2 | Connect 2-wire smoke detectors across zone 1 terminals (10 through 11) as shown in *Figure 6-2*. Observe proper polarity when connecting the detectors. |
| 3 | Connect the EOL resistor across the loop wires **at the last detector.** |

- 2K EOL resistors must be used on fire zones (standard 2K EOL resistors may be used on burglary and panic zones) and must be connected across the loop wires of each zone at the last detector.
- The alarm current provided by zone 1 will support only one smoke detector in the alarmed state.

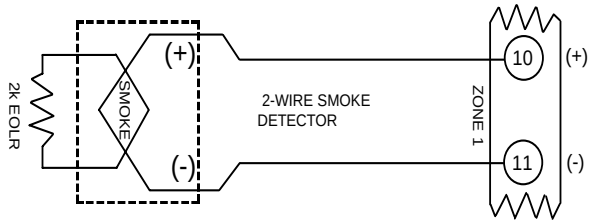



***Figure 6-2: 2-Wire Smoke Detector Connected to Zone 1.***

## Installing 4-Wire Smoke Detectors to Zones 1-8

When programmed for fire warning usage, zones 1-8 can monitor 4-wire smoke detectors, N.O. fire alarm initiating devices, or N.O. sprinkler system supervisory devices.

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 (see the *Final Power-Up Procedure* section for auxiliary power ratings).

Auxiliary power to 4-wire smoke detectors is not automatically reset after an alarm, and therefore must be momentarily interrupted using either an external switch or a 4204 Relay Module.

**UL**

- Power to 4-wire smoke detectors must be supervised with an EOL device (use a System Sensor A77-716B EOL relay module connected as shown in *Figure 6-3*).
- 2-wire smoke detectors may not be used in UL installations.

### Compatible 4-Wire Smoke Detectors

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

| | |
|---|---|
| Photoelectric, direct wire | System Sensor 2412 |
| Photoelectric w/heat sensor, direct wire | System Sensor 2412TH |
| Ionization, direct wire | System Sensor 1412 |

### Wiring 4-wire Smoke Detectors

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

| Step | Action |
|---|---|
| | Select from the list compatible 4-wire smoke detectors. |
| 2 | Connect detectors (including heat detectors, if used) across terminals of the zone selected. All detectors must be wired in parallel. See *figure 6-3.* |
| 3 | Connect the EOL resistor across the loop wires **at the last detector.** |

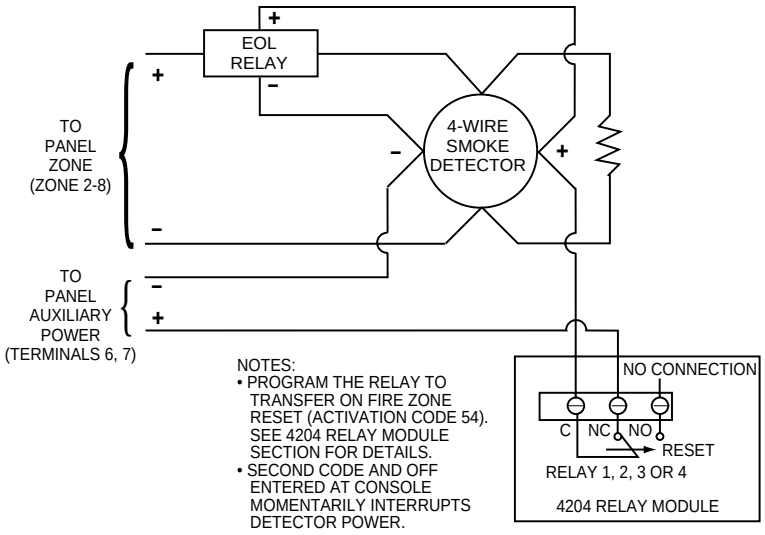



***Figure 6-3: 4-Wire Smoke Detector Connections (Zones 1-8)***

## Installing 2-Wire Latching Glassbreak Detectors to Zone 8

Use zone 8 for connection of compatible 2-wire latching-type glassbreak detectors. After an alarm, the first code + OFF turns off the siren and disarms the system; the second code + OFF clears the memory of alarm and resets the glassbreak detector.

### Compatible Glassbreak Detectors

Use detectors that meet the following ratings:

| | |
|---|---|
| **Standby Voltage:** | 5VDC–13.8VDC |
| **Standby Resistance:** | Greater than 20k ohms (equivalent resistance of all detectors in parallel) |
| **Alarm Resistance:** | Less than 1.1k ohms (see note below) |
| **Alarm Current:** | 2mA–10mA |
| **Reset Time:** | Less than 6 seconds |

The IEI 735L Series detectors have been tested and found to be compatible with these ratings. You can use up to 50 IEI 735L Detectors connected in parallel.

You can use detectors which exceed 1.1k ohms in alarm, provided they maintain a voltage drop of less than 3.8 volts in alarm.

- The alarm current provided by zone 8 will support only one glassbreak detector in the alarmed state.
- Do not use other N.O. or N.C. contacts when using glassbreak detectors on zone 8. Other contacts may prevent proper glassbreak detector operation.

### Wiring 2-wire Glassbreak Detectors

To wire 2-wire glassbreak detectors, perform the following steps:

| Step | Action |
|---|---|
| | Select from the list compatible 2-wire latching glassbreak detectors. |
| 2 | Connect detectors across zone 8 (terminals 21 and 22). See *Figure 6-4.* |
| 3 | Connect the EOL resistor across the loop wires **at the last detector.** |

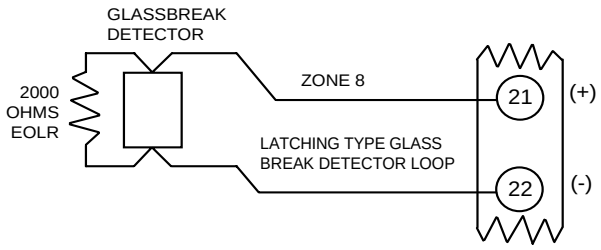



***Figure 6-4. Wiring Latching Glassbreak Detectors to Zone 8***

# 2-Wire Polling Loop Expansion

### In This Section



## Polling Loop Overview

You can expand the system from the basic 9 zones to up to 128 zones using the built-in 2-wire polling loop. Each device that is connected to the polling loop has the capability to communicate with the panel about its status. These devices are called RPMs (Remote Point Modules). The polling loop:

- Provides both power and data to the RPM zones
- Constantly monitors the status of all zones enabled on the loop
- Provides maximum current draw for all devices on the polling loop of 128mA (unless using a 4297 Polling Loop Extender Module).

## Common Characteristics of Polling Loop Zones

Polling loop zones have the following characteristics:

- Must use RPM (Remote Point Module) devices
- Supervised by control panel
- Individually assignable to one of 8 partitions
- Polling loop smoke detector LED will latch on the first detector to go into alarm. Clearing alarm memory clears the latched LED.
- Polling loop smoke detector LED periodically flashes to indicate communication with the control.

## Installing RPM Devices

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 from the control panel in a star configuration as shown in *Figure 7-1*.

Although each polling loop device is wired in parallel, each device has its own unique zone number (or group of zones if it is a zone expansion device). On some devices, this is determined by the setting of DIP switches. Other devices have a built-in unique serial number which must be "learned" into the control as the zone number desired.

**UL**

- The 4208 must be mounted either inside the VISTA-128B cabinet or in a separate enclosure which has a tamper-supervised cover.
- The 4190WH right loop must not be used, and the left loop must be EOLR-supervised.
- The 4278 Auxiliary Sensor Loop cannot be used.
- The 4194 is not UL Listed.
- The 4297 must be powered from the VISTA-128B Auxiliary Power Output or from a UL Listed supplementary power supply.

### Compatible Polling Loop Devices

| | | |
|---|---|---|
| **4208** | **8-Zone Expander** | • Accommodates up to 8 zones via the polling loop.<br>• DIP switch-programmable.<br>• The first two zones can be either normal or fast response (DIP switch selectable).<br>• All zones are EOLR-supervised (first six zones = 4.7k ohms; last two zones = 30k ohms), provided with the 4208. |
| **4190WH** | **2-Zone Expander** | • Accommodates up to 2 zones via the polling loop.<br>• DIP switch-programmable.<br>• The left zone can be EOLR-supervised (required in UL installations), can accept either open or closed circuit sensors, and can be set for fast response.<br>• The right zone is unsupervised and can accept closed circuit sensors only (cannot be used in UL installations). |
| **4278** | **Quad PIR** | • Quad element PIR with built-in RPM (connects directly to the polling loop).<br>• DIP switch-programmable.<br>• Includes mirrors for both wide-angle and curtain/long-range applications.<br>Features a nonsupervised auxiliary sensor loop that can accept closed circuit sensors only (cannot be used in UL installations). |
| **4275** | **Dual PIR** | • Dual-element PIR with built-in RPM (connects directly to the polling loop).<br>• DIP switch-programmable.<br>• Includes mirrors for both wide-angle and curtain/long-range applications and can use the 1875PA Pet Alley mirror.<br>• Built-in selectable pulse count capability. |
| **4194** | **Surface Mount Reed Contact (Wide Gap)** | • Wide-gap, surface-mounted reed contact with built-in RPM (connects directly to the polling loop).<br>• DIP switch-programmable. |
| **4192SD** | **Photoelectric Smoke Detector Devices** | • One-piece photoelectric smoke detector with built-in RPM.<br>• DIP switch-programmable. |
| **4192SDT** | **Photoelectric Smoke Detector w/Heat Detector** | • One-piece photoelectric smoke detector with 135°F (57°C) heat detector and built-in RPM.<br>• DIP switch-programmable. |
| **4192CP** | **Ionization Smoke Detector** | • One-piece products of combustion ionization detector with built-in RPM.<br>• DIP switch-programmable. |

### Compatible Polling Loop Devices

| | | |
|---|---|---|
| **4101SN** | **Serial Number Single Output Relay Module** | • Form C relay rated at 2A, 28VAC/VDC with contact supervision.<br>• One class B/style B EOLR-supervised aux input zone.<br>• Serial Number ID learned by control panel.<br>• Tamper-protected cover. |
| **4939SN-BR**<br>**4939SN-GY** | **Serial Number Surface Mount Reed Contacts** | • Compact surface-mount magnetic reed contact with built-in RPM.<br>• Serial number ID learned by control panel. |
| **4191SN-WH** | **Serial Number Recessed Reed Contact** | • Recessed (1/2" dia.) magnetic reed contact with built-in RPM.<br>• Serial number ID learned by control panel. |
| **4959SN** | **Aluminum Overhead Door Contact** | • 24-inch armored cable<br>• Serial number ID learned by control panel. |
| **4208U** | **Universal 8-Zone Expander** | • Uniquely identifies 8 EOLR supervised zones (all zones use 10k resistors, supplied).<br>• Can be used in zone assignment mode or serial number mode.<br>• When used in the serial number mode, each serial number in the selected group can be assigned to any zone number.<br>• Loops A&B can be programmed for fast (10msec) response.<br>• Can be optionally powered from an external DC power supply to reduce current draw from the polling loop.<br>• Tamper protected |
| **4193SN** | **Serialized 2-Zone Expander** | • Two-zone expander used to connect alarm sensing devices to control panels.<br>• Can be configured as one supervised zone (10K EOLR) and one unsupervised zone, or two unsupervised zones (normally closed devices only).<br>• Serial number ID learned by control panel. |
| **4293SN** | **Serialized 1-Zone Expander** | • Single-zone expander used to connect alarm-sensing devices to control panels.<br>• Can be configured as one unsupervised zone (normally closed devices only).<br>• Serial number ID learned by control panel. |
| **7500** | **Single Technology Glass Break Detector** | • Glassbreak detector with built-in RPM.<br>• DIP switch programmable. |
| **9500** | **Dual Technology Glass Break Detector** | • Dual technology glass-break detector with built-in RPM<br>• DIP switch programmable. |

**UL** Models 7500 and 9500 glassbreak detectors are not UL Listed.

### Wiring Polling Loop Devices

When running polling loop wires, they must not be run within 6" of AC power, telephone, or intercom wiring. Since the polling loop is carrying data between the control panel and the devices, interference on this loop can cause an interruption of this 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.)

To wire the polling loop devices, perform the following steps:

| Step | Action |
|---|---|
| | Select from the list compatible polling loop devices. |
| 2 | Run wires to each device on the polling loop. No individual wire run may exceed the lengths given in the table to follow. In addition, no more than 64mA may be drawn on any individual wire run. When a star configuration is used, the total length of all wire runs combined cannot exceed 4000 ft (2000 ft. if using unshielded wire in conduit or shielded wire). Twisted-pair is recommended for all normal wire runs. |
| 3 | Wire each device to the polling loop, making sure to use correct polarity when making connections (refer to the device's instructions). |
| 4 | **If you are using serial number devices,** and intend to have the control enroll each serial number 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.<br>**Note:** If you intend to manually enter the serial numbers through the keypad or through Compass downloading software, all the devices may be connected before powering up to program. |
| 5 | **If you are using devices with DIP switches**, set each device's DIP switches for the zone number you are assigning it. Refer to the device's instructions or the DIP Switch Tables at the end of this manual when setting addresses. |

**Maximum Polling Loop Wire Runs**

| Wire Gauge | Max. Length |
|---|---|
| #22 gauge | 650 feet |
| #20 gauge | 950 feet |
| #18 gauge | 1500 feet |
| #16 gauge | 2400 feet |

Certain polling loop devices have a DIP switch which can be used either to select the device's zone number or to select the enrolling of a unique, embedded serial number by the control panel. When used with VISTA-128B, these devices **MUST** be set for the serial number mode of operation.

Be sure to include the total current drawn on the polling loop when figuring the total auxiliary load on the panel's power supply (use the AUXILIARY CURRENT DRAW WORKSHEET in the *Final Power Up Procedure* section.

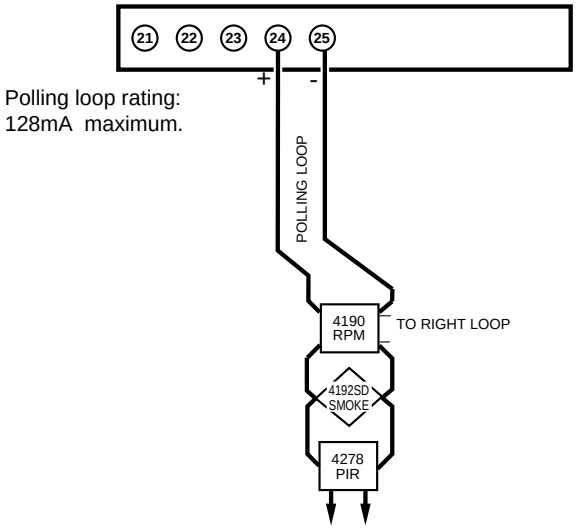
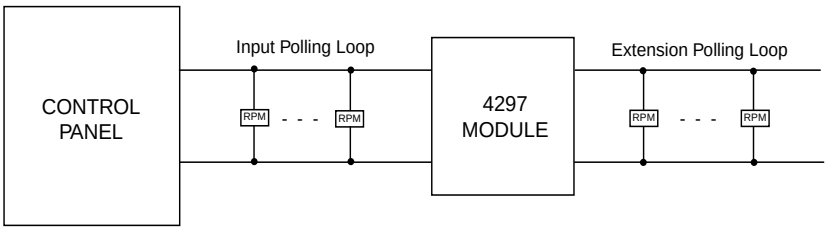



***Figure 7-1: Polling Loop Connections to the VISTA-128B***

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 7-2 and 7-3*, to follow.

**DO NOT** use the 4197 Polling Loop Extender module with the VISTA-128B.

Notes: - Do not use the 4197 module.
- Refer to 4297 instructions for more detailed installation information. The limits shown below supercede the limits described in the 4297 instructions.
- Do not connect 4297 modules in series.




**Input Loop Limits:**
- 128mA max. No more than 64mA on any individual wire run.
- No individual wire run may exceed:

| Gauge | Length |
|---|---|
| #22 | 650 ft. |
| #20 | 950 ft. |
| #18 | 1500 ft. |
| #16 | 2400 ft. |

- Total length of all wire runs combined cannot exceed 4000 ft. (2000 ft. if using unshielded wire in conduit or shielded wire).

**Extension Loop Limits:**
- Same as for the input polling loop.

**Combined Input and Extension Polling Loop Limits:**
- No more than 119 devices combined.
- Total length of all wire runs on all loops combined cannot exceed 6400 ft. (3200 ft. if using unshielded wire in conduit or shielded wire)

***Figure 7-2: Polling Loop Connections Using One 4297 Extender Module***

Notes: - Do not use 4197 module.
- Refer to 4297 instructions for more detailed installation information.
  The Limits shown below supercede the limits described in the 4297 instructions.
- Do not connect 4297 modules in series.

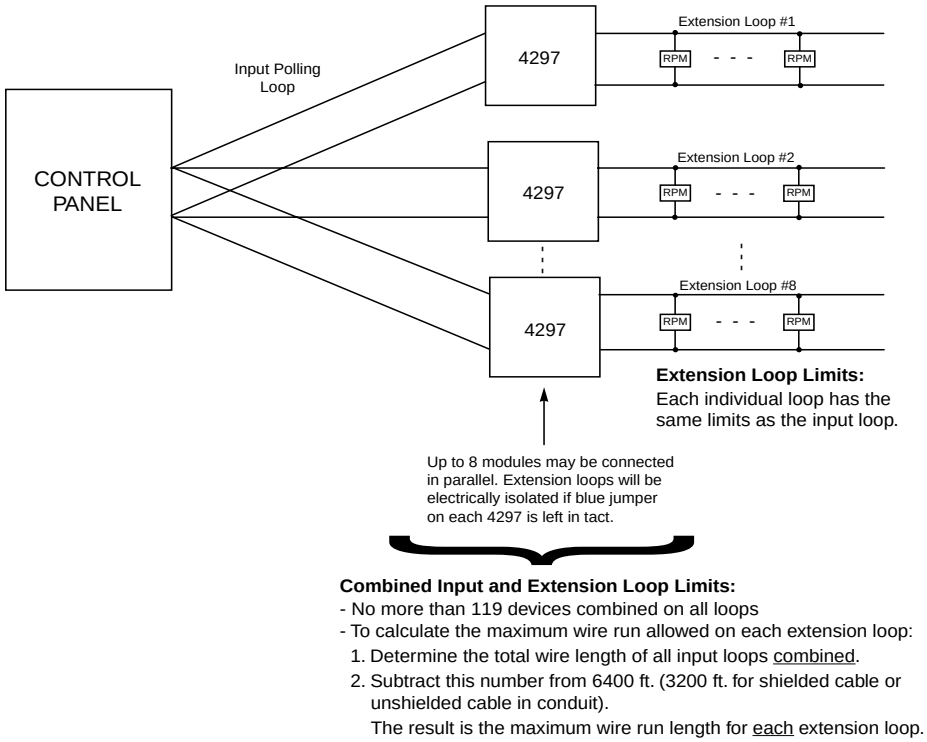



***Figure 7-3. Polling Loop Connections Using Multiple Extender Modules***

**Note:** The input loop limits stated in *Figure 7-2* apply to *Figure 7-3* as well.

## Polling Loop Supervision

A short on the polling loop is indicated by a trouble on its supervisory zone and reports as a trouble condition only. As such, a polling loop should be assigned zone type 05 if annunciation as a trouble condition is desired.

If a device on the polling loop fails (the panel cannot "see" that device), the partition or partitions that use that device will display a trouble condition for all zones associated with that device. If the panel is armed when a device fails, and the zone is programmed as a burglary type, that device will cause an alarm on the corresponding partition(s). Otherwise the zone will generate a trouble condition.

A trouble on zone 997 will not prevent a partition from being armed, as long as all polling loop zones on that partition are bypassed.

# Wireless Zone Expansion

### In This Section



## Common Characteristics of Wireless Zones

- Supervised by control panel for check-in signals (except certain nonsupervised transmitters)
- Individually assignable to one of 8 partitions
- Individually assignable to access points

**UL** Wireless devices may not be used in UL Commercial Burglary installations.

The following receivers may be used and supports the number of zones shown below:

**5800 Series Receivers**

| Recvr | Zones |
|---|---|
| 5881L | up to 8 |
| 5881M | up to 16 |
| 5881H | up to 128 |

In Canada, 5800 systems must use 5882 Series receivers: 5882L/5882H. Information in this manual relative to the 5881 Receivers applies as well to the 5882 Receivers. 5881 and 5882 Receivers can all use the same transmitters.

## RF System Operation and Supervision

- The receiver responds to status and alarm signals from wireless transmitters (at 345MHz USA; 315MHz in Canada) within a nominal range of 200 feet, and relays this information to the control.
- Each supervised transmitter sends a supervisory signal to the receiver every 70-90 minutes. If, after a programmed interval of time (e.g., 12 hrs), the receiver does not hear from a *particular* transmitter, the word “CHECK” or “TRBL” will appear at the corresponding partition’s keypad(s) accompanied by the zone number in question. The trouble will not prevent you from arming the panel, but the zone must first be bypassed.

- 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. If, within a programmed interval of time (defined by program field 1*30), the receiver does not hear from *any* of its transmitters. A "CHECK" or "TRBL" message will appear for zones 988 (2nd receiver) or 990 (1st receiver) if response type 05 is assigned to these supervisory zones and if programmed, Contact ID event code 333 is sent to the central station. This message is an indication that the RF receiver is "deaf." The fault may be accompanied by a supervision fault for one or more RF transmitters.
  2. If, the receiver has detected a condition that may impede proper RF reception (i.e., jamming or other RF interference). The control checks the receiver for this condition every 45 seconds. A "CHECK" or "TRBL" message will appear for zones 988 (2nd receiver) or 990 (1st receiver) if response type 05 is assigned to these supervisory zones and if programmed, Contact ID event code 344 is sent to the central station

---

**UL** A response type must be programmed for zones 990 (1st receiver) and 988 (2nd receiver) if being used, for UL commercial fire and burglary installations.

---

- The control checks the receiver connections about every 45 seconds. If the panel has lost communication with the receiver, a "CHECK" or "TRBL" message will appear for the respective receiver supervisory zone (8 + 2-digit receiver device address; for example, Device address 05 = supervisory zone 805). Supervisory zones must be programmed for Day/Night (type 05). The "CHECK" or "TRBL" display may be an indication that the wiring to the receiver is incorrect, or that the DIP switches are not set for the same address the receiver was assigned to in the control's *Device Programming* in the *#93 Menu Mode*.
- Two identical receivers can be used to provide either a greater area of coverage or redundant protection.
- Any zone from 1 to 128 can be used as a 5800 Series wireless zone, with the exception of zone 64 (reserved for a wireless keypad).

## RF System Installation Advisories

- Place the receiver in a high, centrally located area for best reception. Do not place it on or near metal objects. This will decrease the range and/or block transmissions.
- For maximum range, 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:
  - Both must be at least 10 feet from each other, as well as from the control panel and remote keypads.
  - 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.
  - The House IDs must be the same.
  - Using two receivers *does not* increase the number of transmitters the system can support (128 zones using the 5881H, plus a wireless keypad).

## Installation and Setup of the 5881 RF Receivers

To install and setup the 5881 RF Receiver, see to *figure 8-1 and* perform the following steps:

| Step | Action |
|---|---|
| | Mount the receiver. It must be mounted externally to the control and can detect signals from transmitters within a nominal range of 200 feet. Take this into consideration when determining mounting location. |
| 2 | Connect the receiver's wire harness to the keypad terminals (6, 7, 8, 9). Plug the connector at the other end of the harness into the receiver. |
| 3 | Refer to the Installation Instructions provided with the receiver for further installation procedures regarding antenna mounting, etc. |
| 4 | Set the receiver's DIP switches for an address (01-07) which is not being used by another device (i.e., keypads, relay modules, etc.).<br>**Note:** Take note of this address setting, because you will need it when programming the receiver into the system in *Device Programming* in the *#93 Menu Mode.* |

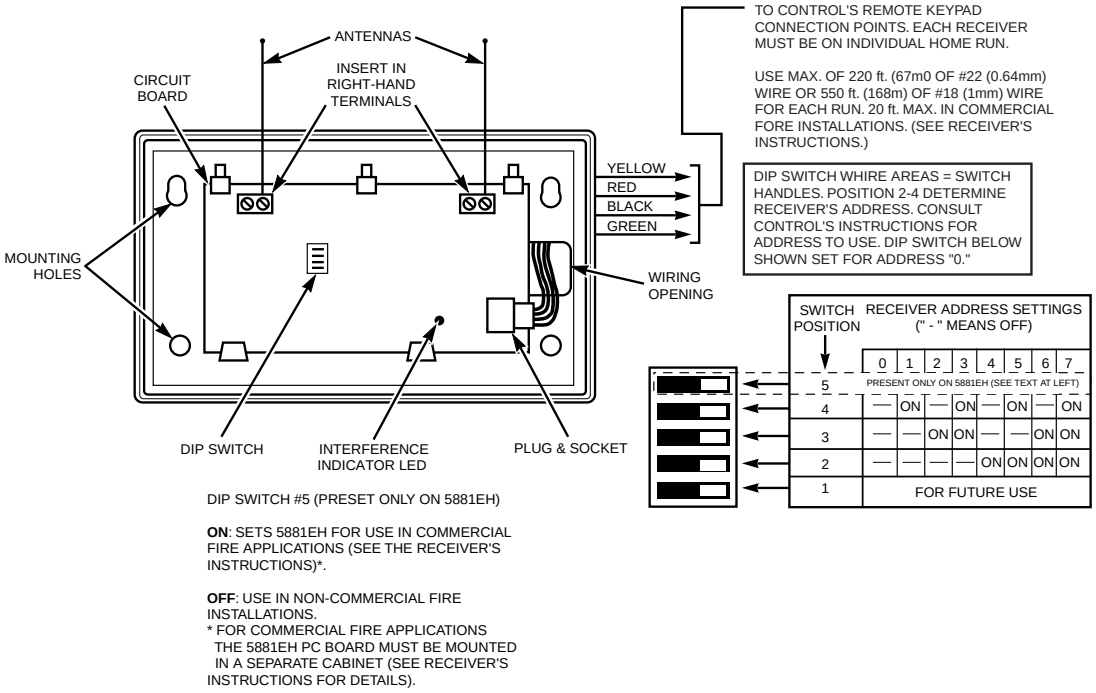



***Figure 8-1. 5881 RF Receiver (cover removed)***

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*.

## Installing the 5800TM Module

Installation of this module is necessary only if you are using one or more 5827BD Wireless Bi-directional keypads.

The 5800TM must be located next to the 5881 Receiver (between one and two feet from the receiver's antennas). The 5800TM must not be installed within the control cabinet. Mount the unit using its accompanying mounting bracket.

### Wiring the 5800TM

To wire the 5800TM,perform the following steps:

| Step | Action |
|---|---|
| 1 | Mount the 5800TM within 2 feet of the 5881 RF Receiver. |
| 2 | Connect the 5800TM to the control panel's keypad connection terminals, using the supplied connector with flying leads, as follows: |
| 3 | Cut the red jumper for Address Setting 28; cut the white jumper for Address 29; cut both jumpers for Address 30. |
| 4 | For additional information, refer to the 5800TM's instructions. |

| WIRE | TERMINAL ON CONTROL |
|---|---|
| RED (+12VDC) | Terminal 6 |
| BLACK (Ground) | Terminal 7 |
| GREEN (Data to Control) | Terminal 8 |
| YELLOW (Data from Control) | Terminal 9 |
| BLUE: Not Used | |

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

## House ID Sniffer Mode

This mode applies only if you are using a wireless keypad (5827/5827BD). Use the House ID Sniffer Mode to make sure you do not choose a House ID that is in use in a nearby system.

To enter this mode, perform the following steps:

| Step | Action |
|---|---|
| 1 | Enter your **[Installer Code] + [#] + [2]**. |
| 2 | The receiver will now "sniff" out any House IDs in the area and display them. Keep the receiver in this mode for about 2 hours to give a good indication of the House IDs being used. Use a House ID that is **not displayed**. |
| 3 | To exit the Sniffer Mode, simply enter your **[Installer Code] + OFF**. |
| 4 | If you need to re-program the House ID of the receiver, do so before proceeding. |

Since 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 built-in serial numbers that must be "learned" by the system using the *#93 Menu Mode Programming*, or input to the control via the downloader. 5800 Series transmitters (except 5827, described separately) do not have DIP switches.

Some transmitters, such as the 5816 and 5817, can support more than one "zone" (referred to as loops or inputs). On the 5816, for example, the wire connection terminal block is Loop 1, the reed contact is Loop 2. Each loop must be assigned a different zone number.

For button-type transmitters (wireless keys), such as the 5804, 5804BD, 5803, and 5801, you must assign a unique zone number to each individual button used on the transmitter. Each button on the transmitter also has a pre-designated loop or input number.

### Transmitter Supervision

Except for some transmitters that may be carried off premises (5802, 5802CP, 5803, 5804, 5827, and 5827BD), each transmitter is supervised by a check-in signal that is sent 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" will be displayed.

The supervision for a transmitter may be turned off by learning it as a "UR" (unsupervised RF) type, as described later in this manual.

Some 5800 Series transmitters have built-in tamper protection and will annunciate a "CHECK" or "TRBL" condition if covers are removed.

### Transmitter Input Types

All of the transmitters described have one or more unique factory-assigned input (loop) codes. Each of the inputs requires its own programming zone (e.g., a 5804's four-button inputs require four programming zones).

Transmitters can be programmed as one of the following types:

| Type | Description |
|---|---|
| **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 be carried off-premises. |
| **BR (Unsupervised Button RF)** | These only send Fault signals. They do not send Low Battery signals until they are activated. The transmitter may be carried off-premises. |

### 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 system can identify a true low battery situation, thus allowing time to arrange a change of battery and maintain protection for that given point within the system.
- Some transmitters (e.g., 5802, and 5803) contain long-life but nonreplaceable batteries. At the end of their life, the complete unit must be replaced (and a new serial number learned by the control).
- Button-type transmitters (e.g., 5801, 5802, 5802CP & 5803) should be periodically tested for battery life.

- Do not install batteries in wireless transmitters until ready to learn. After learning, batteries need not be removed.
- Before mounting transmitters permanently, conduct Go/No Go Tests to verify the signal strength and reorient or relocate transmitters if necessary. See the *Testing the System* section.

## Compatible 5800 Series Transmitters

| Model | Product | Input Type | Description |
|---|---|---|---|
| 5801 | Wireless Panic Transmitter | UR or RF | • Has four pushbuttons, each with a unique input (loop) code.<br>• Programmable responses (e.g., Panic, Arm–STAY, Arm–AWAY, Disarm, etc.<br>• For arming/disarming functions, button must be assigned to a user code when "adding a user." |
| 5802<br><br><br><br>5802CP | Pendant (Personal Emergency Transmitter)<br><br><br><br>Belt Clip (Personal Emergency Transmitter) | BR Only | • Has single pushbutton.<br>• Usually be programmed for response type of 24 Hr. Audible or 24 Hr. Silent (other zone responses are possible).<br>• Contains a nonreplaceable battery. At the end of the battery's life, the entire unit must be replaced.<br>• If using for arming/disarming, the button must be assigned to a user code when "adding a user." |
| 5802MN | Miniature (Personal Emergency Transmitter) | UR or RF | • Has single pushbutton<br>• Usually programmed for a response type of 24 Hr. Audible or 24 Hr. Silent (other zone responses are possible.<br>• If using for arming/disarming, the button must be assigned to a user code when "adding a user."<br>• Contains a replaceable battery. |
| 5804 | Wireless Key Transmitter | BR Only | • Has four pushbuttons, each with a unique input (loop) code.<br>• Programmable responses (e.g., Arm–STAY, Arm–AWAY, Disarm, etc.).<br>• Contains a replaceable battery.<br>• If using for arming/disarming, the button must be assigned to a user code when "adding a user." |
| 5806/5807<br>5808 | Wireless Photoelectric Smoke Detectors | RF | • One-piece smoke detectors with built-in transmitter.<br>• UL Listed for residential fire usage only with VISTA-128B. |

**Compatible 5800 Series Transmitters (cont'd)**

| Model | Product | Input Type | Description |
|---|---|---|---|
| 5816 | Door/Window Transmitter | RF | • Has two unique input (loop) codes: one for a wired closed circuit contact loop; the other for a built-in reed switch (used in conjunction with a magnet). |
| 5817 | Multi-Point Universal Transmitter | RF | • Has three unique input (loop) codes: one for a "Primary" contact loop with programmable options; the others for two "Auxiliary" closed circuit contact loops. |
| 5818 | Recessed Transmitter | RF | • Reed switch magnetic contact sensor that is easily concealed in the frame and edge of a door or window.<br>• Has a unique input (loop) code. |
| 5827 | Wireless Keypad | House ID | • Can be used to turn the burglary protection on and off<br>• Features the same built-in panic functions as wired keypads<br>• The keypad is identified as zone "000" on wired keypads when it transmits with a low battery . |
| 5827BD | Wireless Bi-directional Keypad | House ID | • *(Used with 5800TM Module)*<br>• Operates the system similarly to wired keypads<br>• Can indicate system status via its 3 LEDs and sounder.<br>• Includes 3 panic keys.<br>• House ID must be set.<br>• Requires 5800TM Transmitter Module (must be enabled in #93 Menu Mode –Device Programming and assigned to a partition in 1*48 |
| 5849 | Glassbreak Detector | RF | • Requires both sound and shock of breaking glass to cause alarm to be transmitted.<br>• Has unique input code. |
| 5890 | PIR Detector | RF | • Dual-element passive infrared detector/transmitter with built-in selectable pulse count.<br>• Has unique input code<br>• 3 minute lock-out between fault transmissions to conserve battery life. |

# Output Devices

## In This Section



## General Information

The VISTA-128B supports up to 96 outputs to activate and de-activate as desired. Each device must be programmed as to how to act (ACTION), when to activate (START), and when to deactivate (STOP). Each of these is described later in this section. This is provided by 4204, 4204CF, FSA-8, FSA-24, 4140SN and/or Powerline Carrier devices.

They can be used to:

- Turn lights on and off
- Control sounders
- Control doors
- Give status indications.

### 4204/4204CF Relay Modules

Each 4204 module provides 4 relays with Form C (normally open and normally closed) contacts. Each 4204CF module adds two additional style Y supervised bell outputs to the system. If 4204CF modules are used exclusively, only relays 1 and 3 on each module can be programmed. The other 2 relays (relays 2 and 4) on each module are used for supervision purposes.

### FSA Modules

The 8-Zone LED Fire System Annunciator FSA-8 and 24-Zone LED Fire System Annunciator FSA-24 provide the ability for a fire response unit to identify quickly and easily the point/zone of a fire. These indicators may be used for other functions as well, such as status indication. A maximum of 4 FSA modules, in any combination, can be supported. Each FSA module can support up to 24 LEDs dependent upon model selection.

### 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.

### Powerline Carrier Devices

Powerline Carrier devices are controlled by signals sent through the electrical wiring at the premises via a 4300 transformer. Therefore, if using Powerline Carrier devices, a 4300 transformer *must* be used in place of the regular system transformer.

This section is used to program relays to activate in response to a programmed **condition.** The system can also be programmed to activate relays at specific **times** by using the *#80 Scheduling Menu Mode–Time Driven Events* function.

## Installing the 4204 and 4204CF Relay Modules

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 wire the relay modules, perform the following steps:

| Step | Action |
|---|---|
| 1 | Set the 4204 or 4204CF's DIP switches for a device address between 01-15. See *Figures 9-1 and 9-2.*<br>**Make sure the address is not being used by another device (keypads, RF receivers, etc.).** |
| 2 | Mount the 4204 and 4204CF Modules as per the instructions provided with the modules. |
| 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.<br>**If mounted remotely homerun each module to the control. The table below shows the maximum wire run lengths from the control to each 4204. Refer to the instructions provided with the 4204CF for its maximum permissible wire lengths.** |

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

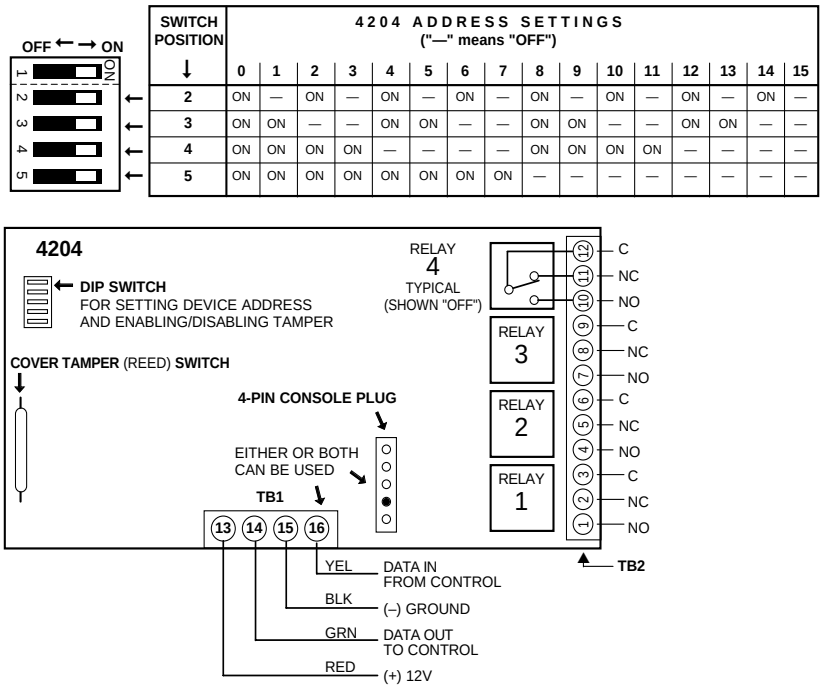



***Figure 9-1: 4204 Relay Module***

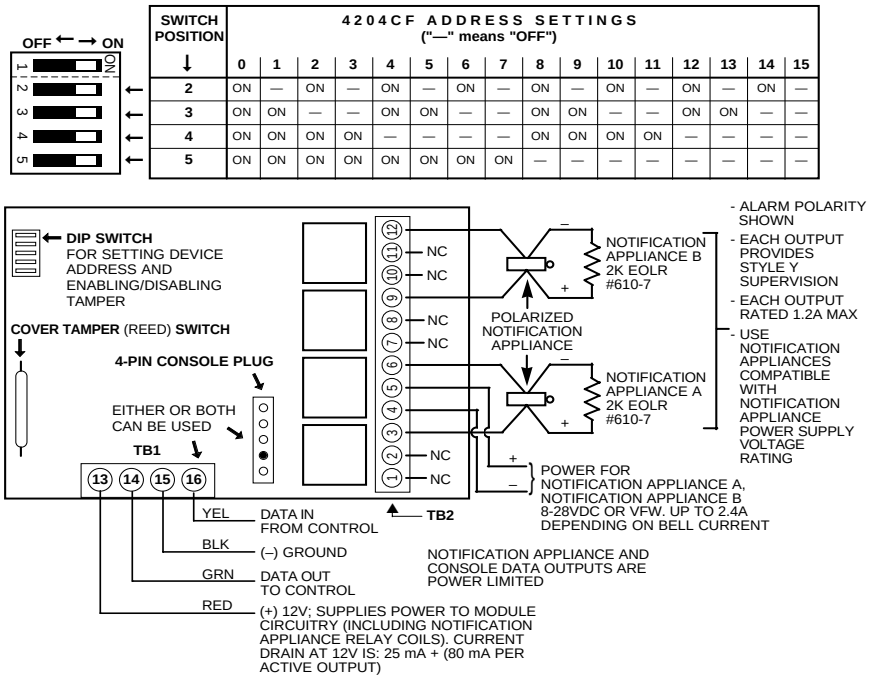



***Figure 9-2: 4204CF Relay Module***

## Installing the FSA Modules

The 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 FSA module, perform the following steps:

| Step | Action |
|---|---|
| 1 | Set the FSA module's DIP switches for a device address between 08-23. See the module's instructions for the DIP switch table.<br>**Make sure the address is not being used by another device (keypads, RF receivers, etc.).** |
| 2 | Mount the FSA module horizontally to a duplex box (quad box for FSA-24). |
| 3 | Connect the module to the control's keypad terminals (6, 7, 8, and 9). |

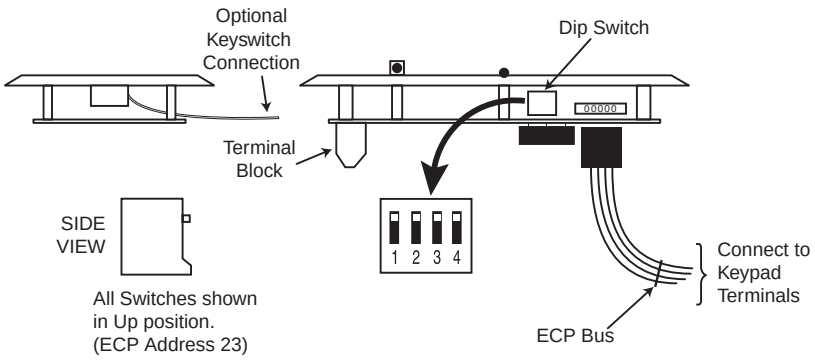



***Figure 9-3: Wiring the FSA Module***

## Wiring the 4300 Transformer

Powerline Carrier devices (such as X-10, ACT, Leviton) 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. They respond to "on" and "off" commands sent from the panel, through the 4300 transformer, to the receiving devices.

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

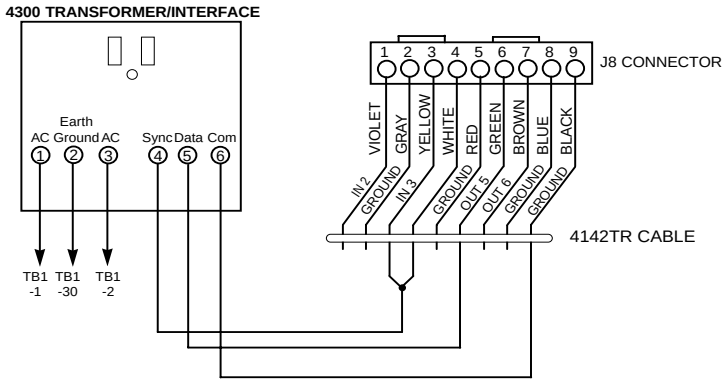



***Figure 9-4: 4300 Wiring Connections***

To connect the 4300 transformer, perform the following steps:

| Step | Action |
|---|---|
| 1 | Run a 6-conductor cable between the 4300 interface and the panel. |
| 2 | Splice a 4142TR cable to the 6-conductor cable. See *Figure 9-4*.<br>**Note that the white and yellow wires of the 4142TR must be spliced together.** |
| 3 | Connect the 4142TR cable to J8 on the control's PC board. |
| 4 | Set the proper House and Unit Codes for each device following the instructions provided with each device. |

## Programming Output Devices

Each output must be programmed to begin one of four types of ACTIONS at a designated START event, and end that ACTION at a designated STOP event.

The letter(s) in parentheses after each function described below, such as (A) after ACTION, are those that appear in the various summary displays of programmed data during programming.

### ACTION (A)

The "ACTION" of the device is how the device will respond when it is activated by the "START" programming. You may want the device to activate momentarily, to pulse on and off continuously, or to remain activated until some other event occurs to stop it.

There are five different choices of actions:

- ACTIVATE for 2 SECONDS and then reset.
- ACTIVATE and REMAIN ACTIVATED until stopped by some other event.
- PULSE ON and OFF until stopped by some other event.
- NO RESPONSE when the device is not used.
- TOGGLE on and off alternately with each activation of event.

### START (STT)

The "START" programming determines when and under what conditions the device will be activated. The following START options are available:

**1) EVENT (EV)** is the condition (alarm, fault, trouble, restore) that must occur to a zone or group of zones (zone list) in order to activate the device. These conditions apply ***only*** when a zone list or zone number is used.

**ZONE LIST (ZL)** is a group of zones to which the "EVENT" applies in order to activate a particular device. Note that there are a total of 15 zone lists that can be programmed; when the selected EVENT (alarm, fault or trouble) occurs in **any** zone in the selected "Start" ZONE LIST (01-15), activation of the selected device will START.

2) **ZONE #** A specific zone going into alarm, fault, trouble, or restore (Event programming) can be used to start the relay action. Enter the 3-digit zone number (000-128).

3) **ZONE TYPE/SYSTEM OPERATION (ZT).** If all zones to be used to start the device have the same response type, and there are no other zones of this type which are **not** to activate this device, then "ZONE TYPE" may be used instead of using a "ZONE LIST" and "EVENT" to activate the device.

   If a System Operation, such as "DISARMING" or "ANY FIRE ALARM" is to activate the device, the appropriate choice would also be entered under the "ZONE TYPE" option.

   ***The "ZONE TYPE/SYSTEM OPERATION" option functions independently of the "EVENT/ZONE LIST" combination.***

   If a specific "ZONE TYPE" is chosen, any zone of that response type going into alarm, trouble, or fault will cause the device to activate as selected in "ACTION." If the same "ZONE TYPE" is also chosen for the STOP programming, any zone of that type that *restores* will de-activate the device.

   If a "SYSTEM OPERATION" is chosen, that operation will cause the device to activate as selected in "ACTION." The different choices for "ZONE TYPE" and "SYSTEM OPERATION" are listed in "Programming Relays" later in this section, and on the Programming Form.

4) **PARTITION No. (P).** The device's "Start" ZONE TYPE/SYSTEM OPERATION may be limited to an occurrence on one partition (1-8), or any partition (0).

### STOP (STP)

The "STOP" programming determines when and under what conditions the device will be de-activated. The following options are available:

1). **RESTORE ZONE LIST (ZL)**. If a "ZONE LIST" is used as the "Stop" event, the device will de-activate when **all** the zones in that list restore from a previous fault, trouble, or alarm condition. This will occur regardless of what is programmed to "START" the device; therefore, a "RESTORE ZONE LIST" would normally only be used when a "ZONE LIST" is used to start the device.

2). **ZONE TYPE/SYSTEM OPERATION (ZT).** Instead of using a "RESTORE ZONE LIST," a specific zone (response) type or system operation action can be selected to de-activate the device.

   If a specific "ZONE TYPE" is chosen, any zone of that response type that restores from a previous alarm, trouble, or fault condition will cause the device to de-activate.

   If a "SYSTEM OPERATION" is chosen, that operation will cause the device to de-activate. The different choices for "ZONE TYPE" and "SYSTEM OPERATION" are listed in "Programming Relays" later in this section, and in the Programming Form.

3) **PARTITION No. (P).** The device's "Stop" Zone Type/System Operation may be limited to an occurrence on one partition (1-8), or on any partition (0).

   ***The "ZONE TYPE/SYSTEM OPERATION" option functions independently of the "RESTORE/ZONE LIST" combination.***

   *See the Programming Guide for a detailed explanation and the display prompts for programming output devices.*

# 4285/4286 VIP Module

### In This Section



**UL** The 4285/4286 VIP Module is not permissible for UL commercial burglary installations.

## General Information

The 4285/4286 VIP Module is an add-on accessory that permits the user to access the security system (and relays) via a TouchTone telephone, 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 the *#93 Menu Mode*, and must be assigned to a partition.

The 4285/4286 VIP Module offers the following 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 Programming* section.
- Can be supervised for connection to control panel (annunciated and reported as Zone 804).

Detailed operating instructions for phone access to the security system are provided with the VIP Module. In addition, a ***Phone Access User's Guide*** is supplied with the VIP Module for the user of the system.

## Mounting the VIP Module

The VIP Module may be mounted in the control cabinet if space is available or, if this is not possible, on the side of the cabinet or adjacent to it. Pry off the VIP Module's cover prior to wiring.

Do not mount the VIP Module on the cabinet door or attempt to attach it to the PC board.

To mount the VIP module, perform the following steps:

| Step | Action |
|---|---|
| 1 | If you are mounting 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. |
| 2 | If you are mounting the VIP module outside the control cabinet, use the screw holes at the rear to mount horizontally or vertically (2-faced adhesive tape may be used, if preferred). You can bring wires out from the side or back (a round breakout is also available on the back). When you complete the Module's mounting and wiring, you should install the module's cover (with label affixed, as indicated next). |
| 3 | Affix the 4285/4286 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. |

## Wiring the VIP Module

The 4285/4286 is wired between the control panel and the premises' handset(s). 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.

To wire the VIP module, perform the following steps:

| Step | Action |
|---|---|
| 1 | 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 see *figure 10-1*. These are the same connections as for remote keypads. |
| 2 | Insert the keyed connector into the mating header on the VIP Module. |
| 3 | Connect terminals 1 through 7 on the VIP Module as shown in the table below. |

| 4285/4286 Terminal | Connects to: |
|---|---|
| **1.** Phone In (Tip) | green wire of direct connect cord |
| **2.** Phone In (Ring) | red wire of direct connect cord |
| **3.** Phone Out (Tip) | brown wire of direct connect cord |
| **4.** Phone Out (Ring) | gray wire of direct connect cord |
| **5.** No Connection | |
| **6.** Audio Out 1* | Speaker |
| **7.** Audio Out 1* | Speaker |

*Supported by the 4286 only

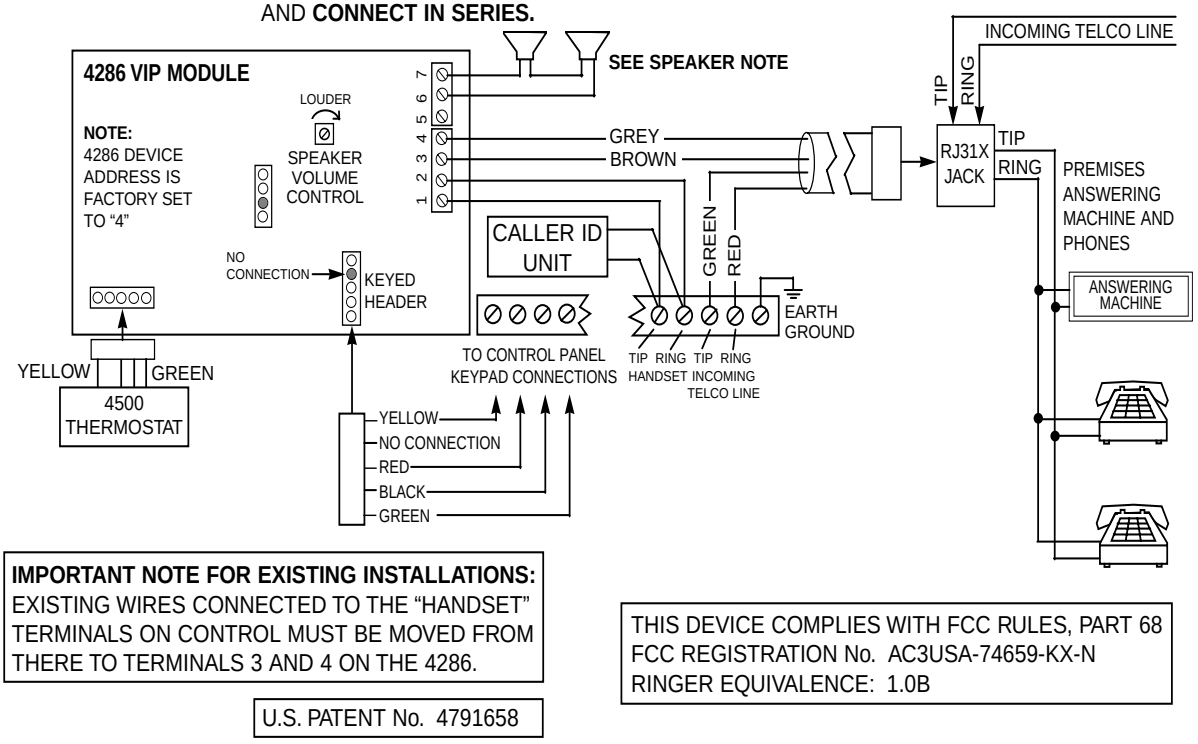



***Figure 10-1: 4285/4286 VIP Module Connections***

Use an RJ31X Jack with the phone cable supplied with the control. Use an additional RJ31X Jack and a direct-connect cord to make connections to the 4285/4286. Make all connections exactly as shown in *Figure 10-1*. This is essential, even if the system is not connected to a central station. **The 4285/4286 will not function if this is not done.** If the leads on the cable are too short to reach their assigned terminals, splice additional wires to them, as required.

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 4285/4286.

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

# Audio Alarm Verification (AAV) Unit

### In This Section



**UL** The Audio Alarm Verification (AAV) feature is not UL Listed.

## General Information

An Audio Alarm Verification (AAV) Module (also known as two-way voice), such as the Eagle 1250, is an add-on accessory that permits voice dialog between an operator at a central station and a person at the alarm installation, for the purpose of alarm verification. This feature is supported only if Alarm reports are programmed to be sent to the primary phone number.

Make connections from Eagle 1250 Module terminals 7 and 8 to the control's zone 5 terminals 16 and 17. The purpose of this connection is to silence and restore the sounders at the premises. It is also used to postpone noncritical dialer reports while the AAV session is in progress. Note that zone 5 is then no longer available as a protection zone. When using the AAV, zone 5 must be assigned a zone response type (e.g., response type 10), and option 1*60 must be enabled to silence sounders on the premises.

## AAV Module Operation

After all messages have been sent during a reporting session to the primary phone number, the control will trigger the AAV if at least one of the messages was an Alarm report. If Contact ID format is selected for the primary phone number, the control will send a Listen-in to Follow message (Event Code 606), which signals the 685 (rev. 4.6 or higher) to hold the phone connection for 1 minute.

Once triggering occurs, the control will give up the phone line to the AAV Module, without breaking connection with the central station. During the time the AAV is active, all sirens and all continuous keypad sounds in all partitions will be shut off. When the AAV indicates that the audio alarm verification session is completed, all keypad sounds will be restored. Sirens will be restored if the alarm timeout period has not expired.

As part of its fail-safe software, the control will limit 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 will break the phone connection and send the new Fire Alarm report, then re-trigger the AAV Mode. All other dialer messages triggered during ongoing conversation will be held until either the AAV Module signals that it is inactive, or the 15-minute timeout occurs.

One way to trigger the AAV Module is by selecting option 3 in field 1*46 and make connections as shown in *Figure 11-1*. Field 1*46 can be used to set ground start, remote console sounding, long range radio, or open/close trigger. If any one of these functions are absolutely necessary in a given installation, the alternative AAV trigger method is via the use of a 4204 Relay Module as shown in *Figure 11-2*. If this method is selected, program the start and stop conditions for that relay as choice 60 "Audio Alarm Verification" during *Output Programming* in the *#93 Menu Mode*.

Some AAV Modules allow remote triggering by ring detection at the alarm installation. Please be advised that if this option is selected, it may defeat modem download and 4285/4286 VIP Module remote access capability. The DIP switch settings shown in *Figure 11-1, Figure 11-2, and Figure 11-3* disable remote AAV Module trigger option. The control requires the AAV Module trigger-type as falling edge, which is set in DIP switch settings shown.

- 685 Receiver software must be rev. 4.6 or higher. Earlier versions will not hold the phone line connection.
- 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."

## Audio Alarm Verification Module Connections

Connect the Audio Alarm Verification Module's falling edge trigger input (terminal 5 on Eagle model 1250) to J7 connector trigger output, or to a 4204 relay module, as shown in *Figure 11-1, Figure 11-2, and Figure 11-3.*

- If also using a 4285/4286 VIP Module, be sure to follow the corresponding diagram when making connections.
- If the phone plug is disconnected from the control, the premise’s phones will not operate.

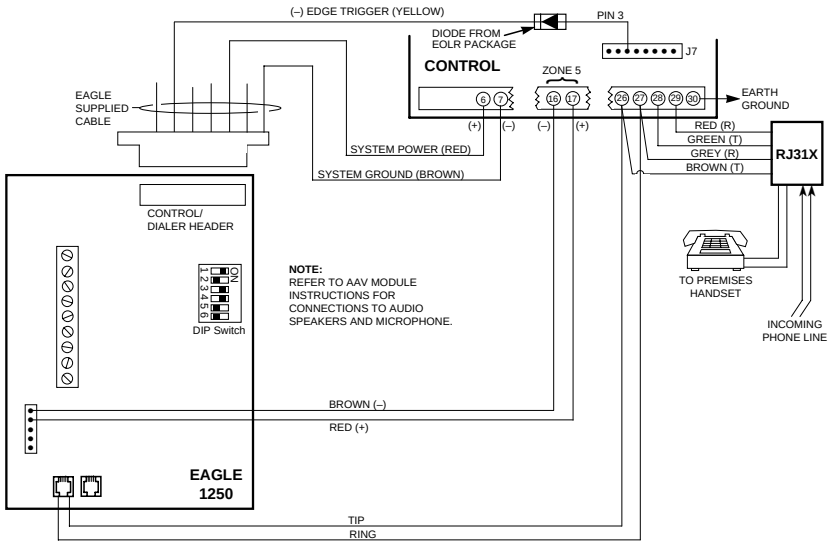



***Figure 11-1: AAV Connections Using the J7 Trigger***

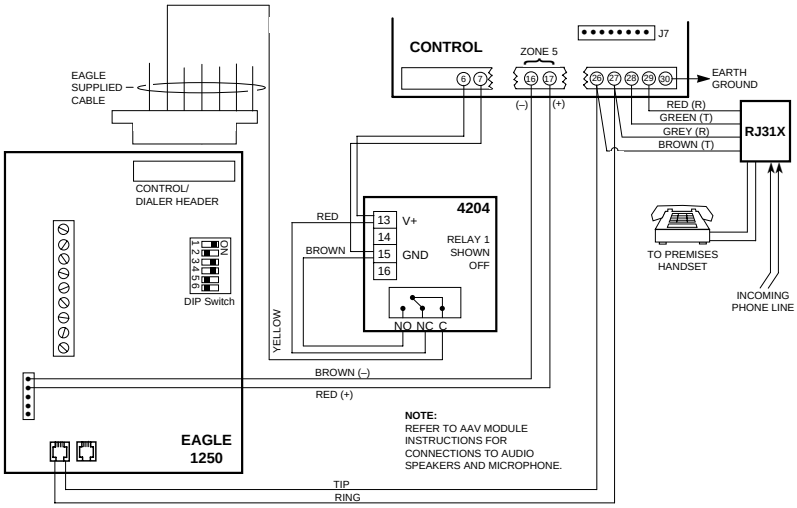



***Figure 11-2: AAV Connections Using a 4204 Relay Module***

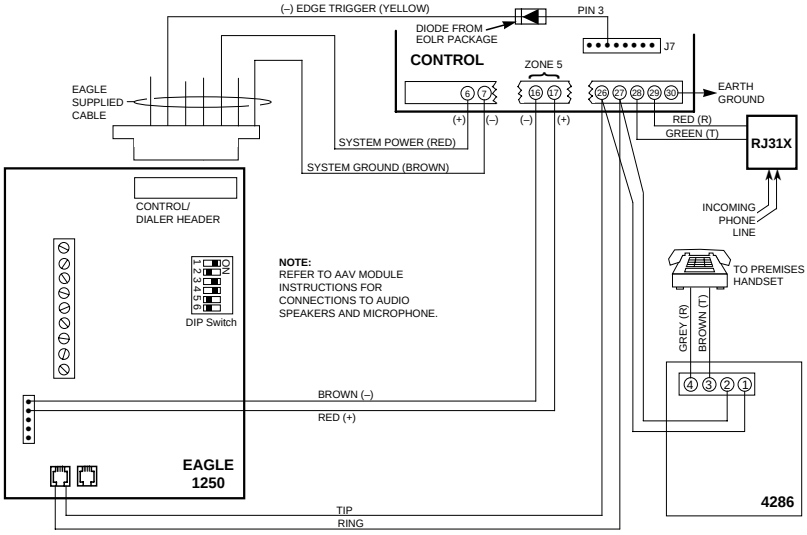



***Figure 11-3: AAV and 4286 VIP Module Connections Using the J7 Trigger***

## Audio Alarm Verification Module Program Options

If you need information about actual programming procedures, see *The Mechanics of Programming* section.

- Program the following data fields:

  ***45** PRIMARY DIALER FORMAT: Set for 1 (Contact ID).

  **1*46** AUXILIARY OUTPUT ENABLE: Set for 3 (unless using 4204 Relay Module).

  **1*60** ZONE 5/AUDIO ALARM VERIFICATION: Set for 1.

Set CANCEL REPORT to a non-zero digit in System Group #1 in *Report Code Programming* in the *#93 Menu Mode.*

- Zone 5 must be programmed for response type 10 and **the EOLR must be removed, regardless of whether or not EOLRs have been enabled in field *41.** Zone 5 is no longer available as a protection zone.
- If using a 4204 relay instead of the J7 trigger, program the relay to trip on Zone Type/Sys. Op. 60 Audio Alarm Verification (see the *Output Devices* section).

# J7 Trigger Outputs

## In This Section



## General Information

The J7 connector, located in the upper right-hand corner of the main PCB, provides 1 input and seven trigger outputs that can be used to interface to the following:

- Ground start module
- Remote keypad sounder
- UL Listed keyswitch
- Audio alarm verification device (two-way voice)
- Auxiliary alarm signaling equipment such as an ADEMCO Long Range Subscriber Radio
- Event logging serial printer (via the 4100SM Interface Module)
- PC computer used to direct-wire download the panel's programming information (via the 4100SM Interface Module)

The trigger output ratings are listed below. Note that all outputs are power-limited.

| | | |
|---|---|---|
| **Output 1:** | LOW: | 2K to ground |
| | HIGH: | 10-14 VDC @ 20 mA max |
| **Remaining Outputs:** | LOW: | 1K to ground |
| | HIGH: | 10-14 VDC through 5K |

The pin assignments for the J7 connector are shown in *Figure 12-1*. Use a 4142TR 9-wire trigger cable (1 supplied) to interface with this connector. The panel does not supervise field wiring connected to this connector.

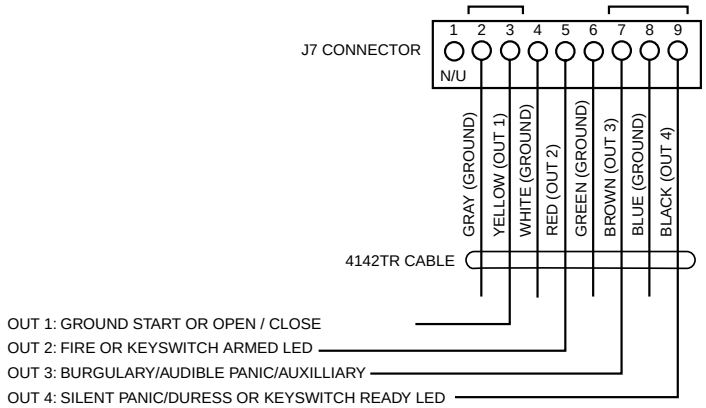



***Figure 12-1. J7 Pin Assignments and Functions***

## Ground Start Operation

**UL** Not intended for use in UL Listed applications.·

You cannot use Output 1 for an Ground Start if using it for a Remote Keypad Sounder, Open/Close trigger, or an AAV module.

Output 1 may be used to trigger an optional 675 Ground Start Module for installations requiring ground start operation instead of loop start operation to obtain dial tone.

When the panel has a message to transmit to the central station, it will seize the line, and then trigger the 675 Module to connect the RING side of the telephone line to earth ground. The panel will cause the module to break the connection between RING and earth ground when it obtains a dial tone.

### Ground Start Operation Setup

To setup the system for ground start operation, perform the following steps:

| Step | Action |
|---|---|
| 1 | Connect the 675 Ground Start Module to the panel's J7 connector trigger output 1, to auxiliary power, and to the RING side of the telephone line, see *figure 12-2*. |
| 2 | Determine which side of the telephone line is the RING side by connecting the (+) lead of a DC voltmeter to earth ground, and the (-) lead to one side of the telephone line. The wire which reads + 50VDC is the RING side. |
| 3 | Program the following data field:<br>**1*46** AUXILIARY OUTPUT ENABLE: Set to "0" (factory default) |

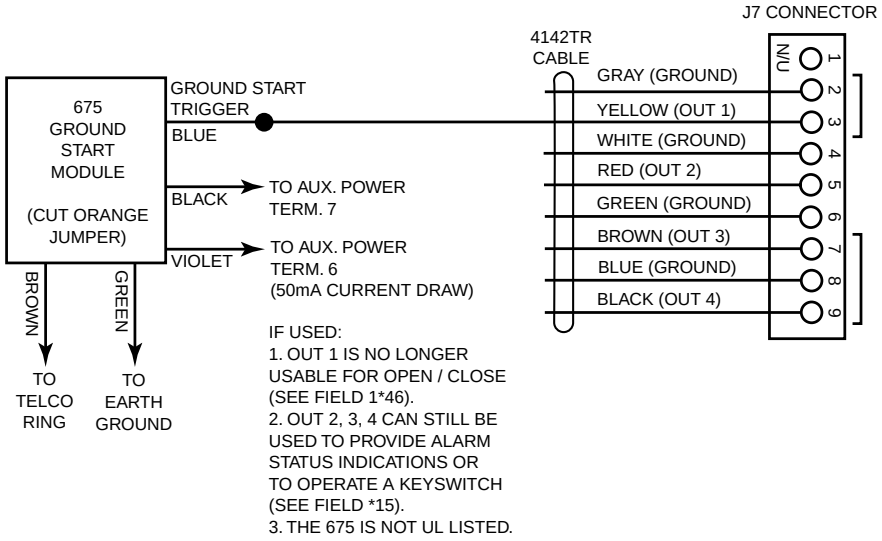



***Figure 12-2: Ground Start Module Connections***

If you need information about actual programming procedures, see: *The Mechanics of Programming* section.

## Remote Keypad Sounder

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, perform the following steps:

| Step | Action |
|---|---|
| 1 | Connect the piezo sounder to the panel's positive auxiliary power output and to Output 1 on the J7 connector as shown in *Figure 12-3*. |
| 2 | Program the following data field:<br>**1*46** AUXILIARY OUTPUT ENABLE: Set to "1" |

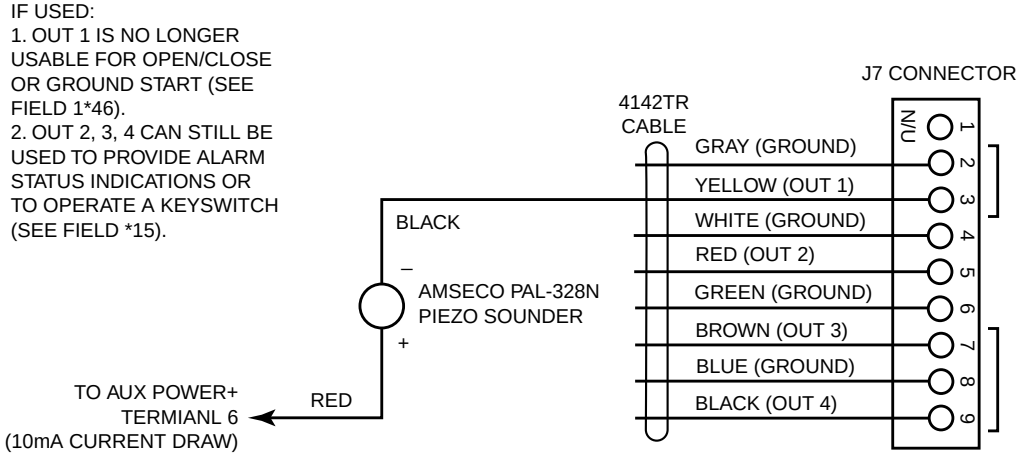



***Figure 12-3: Remote Keypad Sounder Wiring***

## Remote Keyswitch

An optional 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 remotely silencing alarms. The keyswitch can operate in only one particular partition.

### Remote Keyswitch Setup

To setup for a remote keyswitch, perform the following steps:

| Step | Action |
|---|---|
| 1 | Connect the keyswitch as shown in *figure 12-4*. The tamper switch need not be used for fire or UL household burglary installations.<br>For UL commercial burglary installations, the tamper switch must be wired to zone 8, and zone 8 must be programmed for day trouble/night alarm (zone type 5). When the keyswitch is removed from the wall, the tamper switch will open, causing an alarm or trouble on zone 8, and causing the control to disable keyswitch operation until the associated partition is disarmed from a keypad. |
| 2 | Program the following data fields:<br>***15** KEYSWITCH ENABLE: Assign the keyswitch to a partition (1-8).<br>***40** OPEN/CLOSE REPORT ENABLE: Enter 1 to enable.<br>**1*46** AUXILIARY OUTPUT ENABLE: Set to "0" (factory default)<br>***93** ZONE PROGRAMMING: Assigned Zone 7 a non-zero response type. |

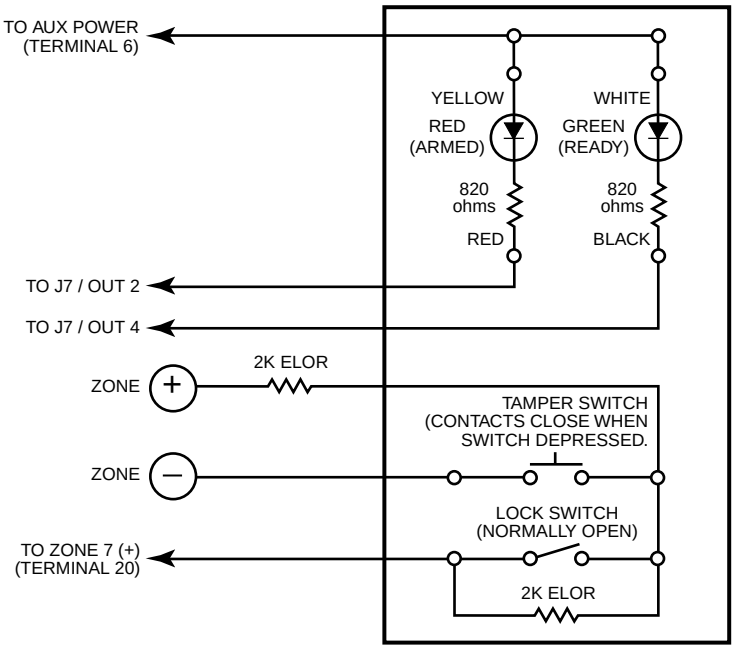



***Figure 12-4: Remote Keyswitch Wiring***

**Keyswitch Operation With System Disarmed and No Alarms Present:**

A momentary short across zone 7 will arm the partition in the AWAY mode, and a short held for more than 10 seconds will arm the partition in the STAY mode. A subsequent short will disarm the partition. The keyswitch LEDs indicate the partition status (see table below).

Faulted zones must either be corrected or bypassed before the system will arm.

**Keyswitch Operation With Alarms Present:**

A momentary short across Zone 7 will silences alarm bell and keypad sounds, and disarms the system if it was armed. The keyswitch LEDs provide a memory of alarm indication (see table below). A subsequent short across Zone 7 will clear the alarm memory indication and reset 2-wire smoke and glassbreak detectors (if used).

**LED INDICATIONS**

| GREEN | RED | MEANING |
|---|---|---|
| OFF | OFF | DISARMED AND NOT READY |
| ON | OFF | DISARMED AND READY |
| OFF | ON STEADY | ARMED AWAY |
| OFF | SLOW FLASH | ARMED STAY |
| OFF | RAPID FLASH | ALARM MEMORY |

If Open/Close reporting for the keyswitch is enabled in field *40, the keyswitch reports as user 0.

## Audio Alarm Verification (AAV) Equipment

An Audio Alarm Verification (AAV) Module (also known as two-way voice), such as the Eagle 1250, is an add-on accessory that permits voice dialog between an operator at a central station and a person at the alarm installation, for the purpose of alarm verification. This feature is supported only if Alarm reports are programmed to be sent to the primary phone number. For a detailed explanation on the operation and wiring of the AAV, see the *Audio Alarm Verification* section.

## Auxiliary Alarm Signaling Equipment

The J7 connector can be used to provide triggers for the following conditions:

- Fire alarm
- Burglary/audible panic alarm
- Silent panic/duress alarm
- Opening/closing (arming/disarming)

These triggers may be used to trip auxiliary alarm signaling equipment such as ADEMCO's 7720, 7720ULF, and 7920SE Long Range Radios.

The open/close, fire alarm, burglary/audible panic alarm, and silent panic/duress alarm triggers are common to all partitions and must be enabled for each partition (data field 2*20). The open/close trigger is LOW when all enabled partitions are armed, and HIGH when any enabled partition is disarmed. The remaining triggers are normally LOW and go HIGH when the corresponding condition occurs in at least one enabled partition. The fire and burglary/audible panic alarm triggers remain HIGH until a [User Code] + OFF is entered in all enabled partition(s) which display these conditions. The silent panic/duress trigger works the same way, except that it is momentary when initiated by duress.

### Wiring Auxiliary Alarm Signaling Equipment

Refer to *Figure 12-5*, *Figure 12-6* and *Figure 12-7* to make connections to the 7720, 7920SE and 7720ULF Long Range Radios.

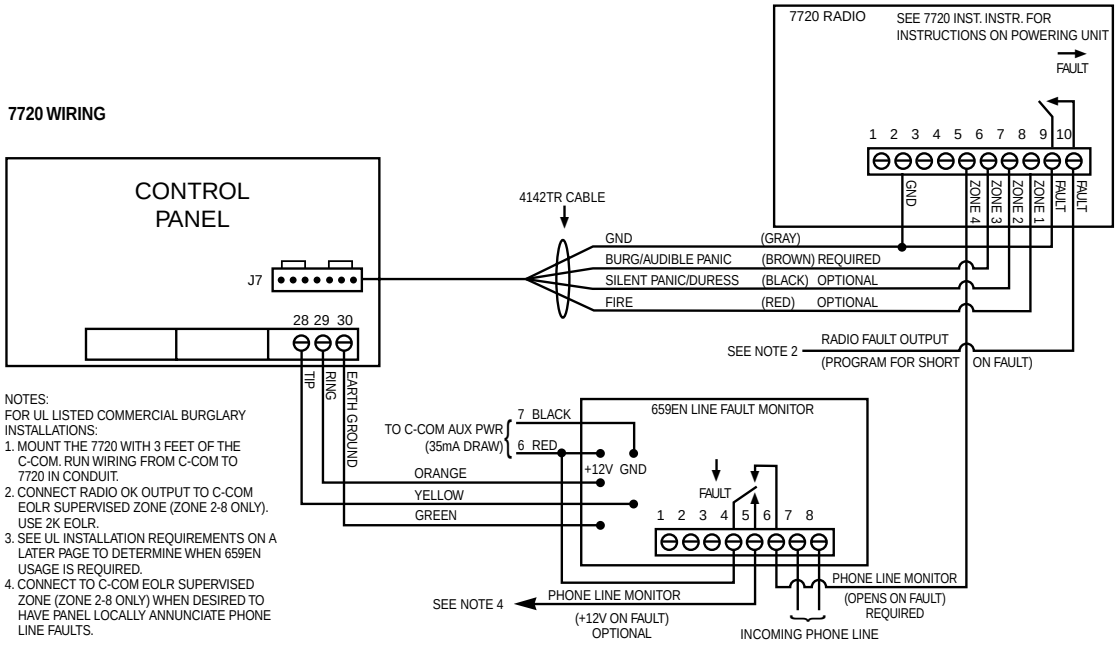



***Figure 12-5: Connections to 7720 Long Range Radios***

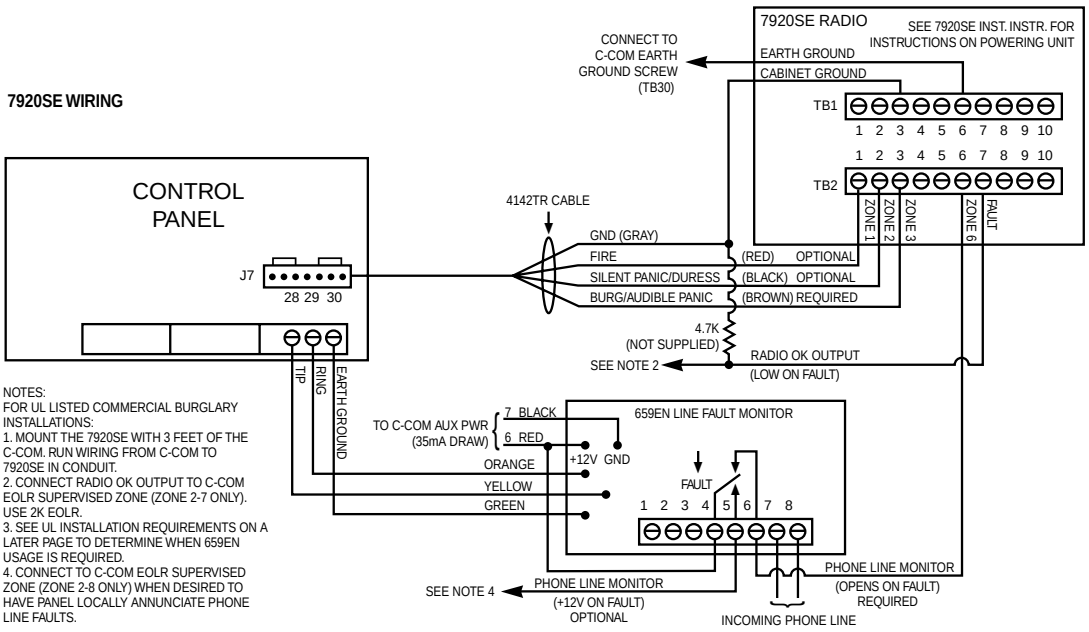
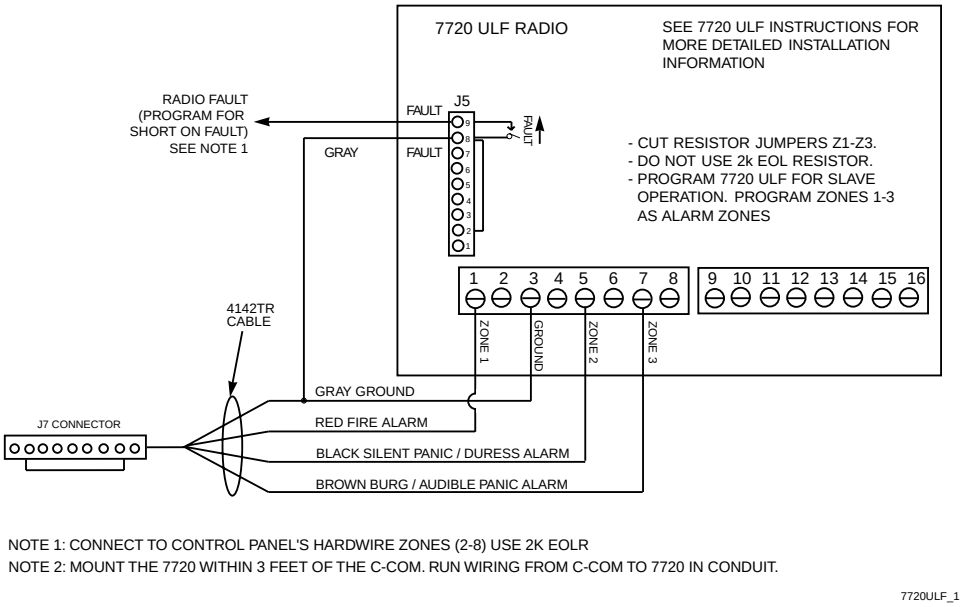



***Figure 12-6: Connections to 7920SELong Range Radios***




NOTE 1: CONNECT TO CONTROL PANEL'S HARDWIRE ZONES (2-8) USE 2K EOLR
NOTE 2: MOUNT THE 7720 WITHIN 3 FEET OF THE C-COM. RUN WIRING FROM C-COM TO 7720 IN CONDUIT.

7720ULF_1

***Figure 12-7: Connections to 7720ULF Long Range Radio***

### Programming for Auxiliary Alarm Signaling Equipment

Program the following data fields:

***15** KEYSWITCH ENABLE: Make sure this field is set to **0**. The keyswitch and the auxiliary alarm signaling equipment cannot be used together.

**1*46** AUXILIARY OUTPUT ENABLE: Set to "0" (factory default)

## Event Log Printer

The VISTA-128B's event log can be printed on a local serial printer.

Connect a UL EDP Listed serial printer to the J8 connector using an ADEMCO 4100SM Interface Module. Refer to *Event Log Options* section for wiring connections, printer configuration, and a description of the keypad commands for event log printing.

# Long Range Radio (ECP)

### In This Section



## General Information

The control can support an ECP Long Range Radio (LRR) (7820, 7835C, and 7845C are supported). These connect to keypad terminals. All messages programmed to be sent via the phone lines may also be enabled to be sent via the LRR. These messages will be transmitted in Contact ID format regardless of the format programmed for the control in fields 45 and 47.

It is recommended that if possible, you use Contact ID format for the main dialer. If Contact ID is not used certain types of reports such as “Listen To Follow” (606), will not be sent at all.

### Supervision

The data lines between the control and the LRR can be supervised, as well as certain functions in the radio. If communication is lost or a trouble condition occurs, both the LRR and the control’s dialer to the central station can be programmed to send a Trouble message.

**Note:** For complete information, see the Installation Instructions that accompany the radio.

### Operation

The LRR reporting options are defined by selecting categories of events for each subscriber ID in fields 58 and 59. The reporting categories are Alarms, Troubles, Bypasses, Openings/Closing, System Events, and Test. In addition, 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 LRR, but Zone 11 will not.

The priority of events from most to least important, transmitted from the VISTA-128B to the LRR is: Fire Alarms, Panic Alarms, Burglary Alarms, Fire Troubles, Non-Fire Troubles, Bypasses, Openings/Closings, Test messages, and all other types of reports when occurring at the same time. Otherwise, messages are transmitted on a “first in/first out” basis.

There are two subscriber ID's programmed into the LRR: 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 LRR will not be transmitted.

If the event is to be reported to both phone numbers, dual reporting, then reporting through the LRR, will be done in an alternating sequence. The first event in the queue will be transmitted to the primary radio central station. Then this event will be transmitted to the secondary radio central station. Once the event is reported successfully via the control’s dialer, it is deleted from the radio’s queue and then the control proceeds to the next event.

If split reporting is selected for the VISTA-128B, then the LRR will follow that option. The radio will send the appropriate reports to the primary and secondary central stations.

## Wiring the Long Range Radio

Connect the data in/out terminals and voltage input terminals of the radio to the control's keypad connection points, terminals 6, 7, 8, and 9, as shown below.

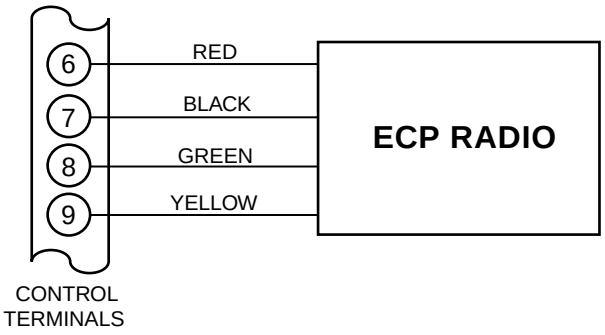



***Figure 13-1. Wiring Long Range Radio to Keypad Terminals***

## Programming for the Long Range Radio

The control's subscriber ID can be passed to the LRR and incorporated into the transmitted data; or the LRR can transmit the subscriber ID programmed in its own EEPROM.

The programming options for the LRR are as follows:

- To send the reports only via the LRR, bypassing the control's dialer (field ∗56).
- To stop transmissions via the LRR if communication via the control's dialer to the central station was successful (field ∗57).
- Selecting categories of events for each subscriber ID. Field ∗58 is for the primary subscriber's ID; field ∗59 for the secondary subscriber's ID. The reporting categories are: Alarms, Troubles, Bypasses, Openings/Closings, System Events, and Tests. The control can be programmed to transmit these reports by partition.

## Trouble Messages

The following messages will be displayed on the 6139 (alpha keypad) when a problem exists the Long Range Radio:

1. "LRR Battery": The battery connected to the radio is low.
2. "PLL out of Lock": The radio 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 radio's EEPROM is corrupt (the internal CRC is bad).

Items 2 and 3 require factory service.

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

Item 6 check the antenna, connection and cable otherwise, this requires factory service.

**NOTE:** All these messages will be displayed in conjunction with the "CHECK 8xx" message which indicates a trouble on the address to which the LRR unit is programmed in the control.

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

# Access Control

### In This Section



**UL** Interfacing the VISTA-128B with the PassPoint Access Control System via the Vista Gateway Module is not permissible for UL commercial burglary installations.

## General Information

The VISTA-128B is capable of utilizing access control operation via one of two methods:

- Interfacing with a VistaKey module
- Interacting with the ADEMCO PassPoint Access Control System (PassPoint ACS) via VISTA Gateway Module.

The VISTA-128B processes fire, burglary, arm, disarm and other information. The VistaKey module and PassPoint ACS process card reader information and control the locking and unlocking of doors.

**DO NOT USE BOTH** the VistaKey and a PassPoint Access Control System on the same alarm panel.

## Access Control Using VistaKey

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

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

**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

VistaKey features are as follows:

- Each VistaKey communicates with the VISTA-128B via a special global polling protocol of the V-Plex polling loop.
- In the event local power to the VistaKey is lost, the VistaKey module provides back-up 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 250 cardholders.
- All configurable options for each VistaKey are accomplished via software, firmware, and non-volatile memory, eliminating the need for PC board jumpers.
- Access Point zone numbers (1-15) are assigned via a user-friendly, 16-position rotary switch.
- The addition and removal of VistaKey modules from the system is easily accomplished via the VISTA-128B keypad.
- Each VistaKey provides one open-collector output trigger (sink 12mA @ 12VDC).

### Mounting and Wiring the VistaKey

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

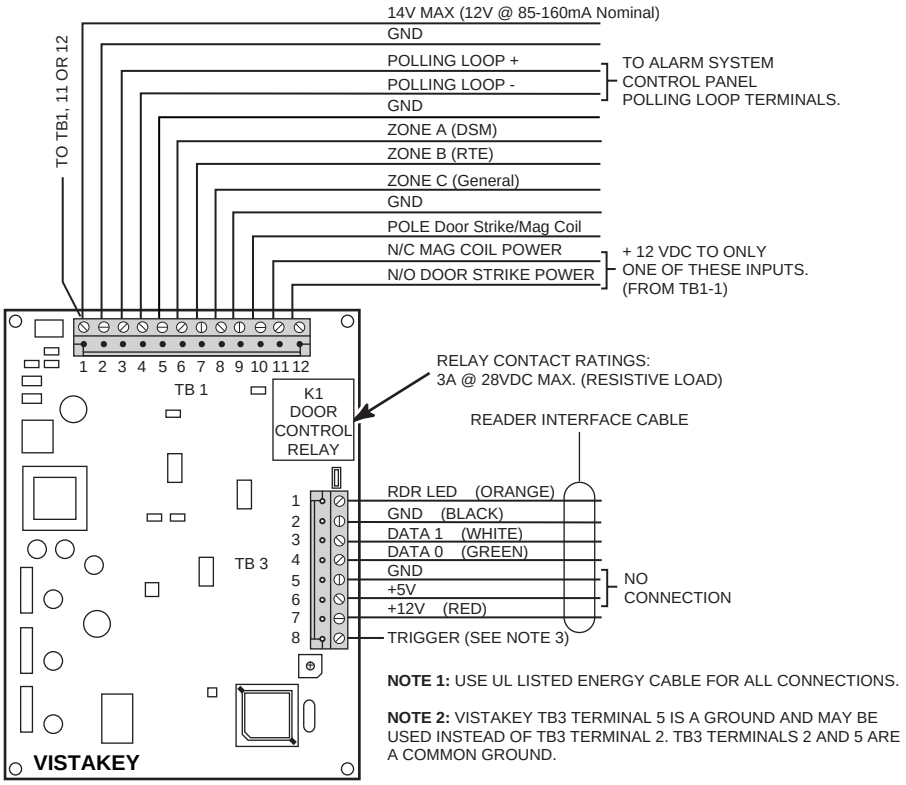
| Step | Action |
|---|---|
| 1 | Mount the VistaKey, Door Strike or Mag Lock, and Card Reader. |
| 2 | If applicable, mount the Door Status Monitor (DSM) and/or Request to Exit (RTE) devices. |
| 3 | Using *Figure 14-1* at the end of this section as a reference, connect the Card Reader interface cable to TB3, *making the +5v or +12v connection last*. |
| 4 | Connect the leads to TB1 in the following order:<br>a. All ground leads to terminals 2, 5 and 9).<br>b. The (optional) DSM, RTE, and General Purpose leads to terminals 6, 7, and 8, respectively.<br>c. Door Strike (or Mag Lock) lead to terminal 10.<br>d. Local +12v or +24v supply lead to terminal 1.<br>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-128B) 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. |

THIS DEVICE COMPLIES WITH PART 15 CLASS A LIMITS OF FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:
(1) IT MAY NOT CAUSE HARMFUL INTERFERENCE.
(2) IT MUST ACCEPT ANY INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

THIS EQUIPMENT SHOULD BE INSTALLED IN ACCORDANCE WITH THE NATIONAL FIRE PROTECTION ASSOCIATION'S STANDARDS 70 & 74 (NATIONAL FIRE PROTECTION ASSOC., BATTERYMARCH PARK, QUINCY, MA. 02269). PRINTED INFORMATION DESCRIBING PROPER MAINTENANCE, EVACUATION PLANNING AND REPAIR SERVICE IS TO BE PROVIDED WITH THIS EQUIPMENT.

FOR ADDITIONAL RATINGS AND SPECIFICATIONS, REFER TO INSTALLATION INSTRUCTION FOR THE VISTAKEY-SK.

WEEKLY TESTING IS REQUIRED TO ENSURE PROPER OPERATION OF THIS SYSTEM.




**NOTE 1:** USE UL LISTED ENERGY CABLE FOR ALL CONNECTIONS.

**NOTE 2:** VISTAKEY TB3 TERMINAL 5 IS A GROUND AND MAY BE USED INSTEAD OF TB3 TERMINAL 2. TB3 TERMINALS 2 AND 5 ARE A COMMON GROUND.

**NOTE 3:** WHEN USING TRIGGER TO TURN ON AN LED OR BUZZER, RETURN HIGH SIDE OF LED OR BUZZER TO TB3 TERMINAL 7. TRIGGER RATING IS 15mA AT 12VDC.

***Figure 14-1: Wiring the VistaKey***

### 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.

### Programming for the VistaKey

The VISTA-128B contains additional programming options in the *#93 Menu Mode* for the VistaKey. See the *VistaKey-SK Installation and Setup Guide* for the detailed programming instructions. These options include:

#### Zone Programming Input Types

- **06 = Serial Number Polling Loop** – (Select for Door Status Monitor Backup DSMB). In the event local power to the VistaKey is lost, the status of the DSM can no longer be reported to the control panel via the normal microprocessor circuits of the VistaKey. In this case a V-Plex SIM, which is located on the VistaKey board and powered directly from the polling loop, is activated 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 (Access Point) must contain the Access Point # (01-15) (address of the VistaKey module).

- **11 = VistaKey Door Status Monitor (DSM)** – This input type is used to define the zone that will monitor when the door (access point) is open. It is used by the system to be able to determine if the door is opened after a card swipe or if the door is being held in an open position. The device is normally a magnetic switch mounted on the door where the status of the switch will be different while the door (access point) is in an open condition.

- **12 = VistaKey Request to Exit (RTE)** – Use this input type to map an uncommitted RTE zone to an alarm panel zone and is not normally used if the zone is used for a request to exit function.

- **13 = VistaKey General Purpose (GP)** – This input type operates in the same manner as other VISTA-128B 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 VISTA–128B control panel.

#### Access Point Programming

This is part of the #93 Menu Mode. It is used to define the parameters for each of the VistaKey access points including which group(s) have access through an access point (door).

#### Access Group Programming

This is part of the #93 Menu Mode. It is used to define the capabilities (privileges) for each group of users.

#### Event/Action Programming

This is part of the #93 Menu Mode. It is used to define events and time windows for a group. This area specifies when a group may be provided entry and/or exit authorization and the action to be taken on entry or exit. This action covers functions such as system arming, system disarming, output activation, and etc.

**Note:**

- Output Device Control may be accomplished via the **[User Code] + [#] + [77]** mode.
- Access Control Test may be accomplished via the **[User Code] + [#] + [78] + [Grant Command]**
- Card enrollment may be accomplished via the **[User Code] + [#] + [79]** mode.

### 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 Using the PassPoint Access Control System

The VISTA-128B interfaces with the PassPoint ACS via the VISTA Gateway Module (VGM). The VGM is connected between the ECP bus (keypad terminals) of the control and the network bus of the PassPoint ACS (see *Figure 14-2*). The control sends the VGM its status information, event log entries and entry/exit requests, (inputs programmed with response type Access Point), from keypads, hardwired zones, and RF transmitters. The VGM then reformats and retransmits this information to the Main Logic Board, (MLB) on the PassPoint ACS network bus.

The VISTA-128B is able to control the following on the PassPoint ACS:

- Access Points

The PassPoint ACS is able to control the following on the VISTA-128B:

- Relays
- Arming/disarming schedules
- Keypad Display

*See the documentation that comes with the PassPoint ACS for details.*

The PassPoint ACS can dedicate some of its inputs for use as regular VISTA-128B hardwired zones (the zone response type is ACS). The PassPoint ACS can also utilize the VISTA-128B's dialer for reports to the central station.

### Using ACS Zone Inputs

If the PassPoint ACS has uncommitted zones, these may be used by the VISTA-128B as hardwired zones.

### Programming the ACS Zone Inputs

| Step | Action |
|---|---|
| 1 | Enter Zone Programming in the #93 Menu Mode. |
| 2 | Program this zone as any other zone. Indicate the input type as ACS (10). |
| 3 | Enter the PassPoint ACS's zone ID (00-31) |

*See Zone Programming in #93 Menu Mode Programming in the Programming Guide for a detailed explanation.*

### PassPoint Dialer Events

All PassPoint ACS events can be sent to the VISTA-128B's dialer via the VGM. These events will also be logged into the control's event log. This is enabled in the PassPoint ACS. *See the PassPoint ACS documentation for a detailed explanation.*

### Wiring the Vista Gateway Module

The Vista Gateway Module is connected between the ECP bus (VISTA-128B keypad terminals) and the network bus of the PassPoint Access Control System. See *Figure 14-2* for the proper wiring connections.

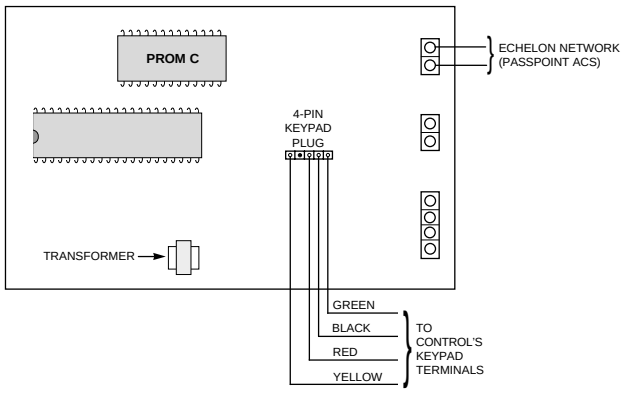



***Figure 14-2: Wiring the Vista Gateway Module***

### Programming the Vista Gateway Module

*See the PassPoint ACS instructions to program the Vista Gateway Module.*

## Access Control of an Entry/Exit Point Using VistaKey or PassPoint

The control can send entry and exit requests to the VistaKey or PassPoint 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

The following entries at the keypad provide access of a door.

- Code + #73
- Code + #74 + access point

  These entries allow a user to gain access to an access point.
- Code + #75 + access point + function

  The selectable functions available are Grant, Protect, Bypass. Selecting "Grant" will temporarily unlock a door. Selecting "Protect" will cause the door to unlock only when a valid keypad entry is received. Selecting "Bypass" will cause the door to be permanently unlocked to allow continuous access.

### Programming the 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 and indicate whether this is an entry or exit console. |
| 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 #93 Menu Mode Programming in the Programming Guide for a detailed explanation.*

### Using an RF Transmitter Zone

A button type RF button-type 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.

An RF transmitter (5816) can be used with a remote switch to provide exit in case of a fire alarm using a PassPoint event action.

#### Programming the RF Transmitter

| 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 (05). |
| 7 | Enter the loop number. |
| 8 | Enroll the serial number |

*See Zone Programming in #93 Menu Mode 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 the *User Access Codes* section for the procedure.
- An RF transmitter will not provide access or grant if the system is in any test mode.

### Using Wireless Keypads

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

#### Programming the Wireless Keypad

Enter the partition the keypad is assigned to in field 1*48.

### 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-128B relays or the ACS relays or triggers are used with keypads and/or RF transmitters whose response type is Access Point (27).

#### Programming the Control of Lighting and Appliances

| 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) (4204/4204CF) or (2) (X-10). |

*See Output Programming in #93 Menu Mode Programming in the Programming Guide for a detailed explanation.*

## Using the VISTA-128B for Stand-alone Access Control

The VISTA-128B can be used for access control without interfacing to PassPoint ACS. A user can trigger an access point (i.e., door strike) for 2 seconds by entering [User Code] + [0].

**Programming the Control for Stand-alone Access Control**

| Step | Action |
|---|---|
| 1 | Enter Output Programming in the #93 Menu Mode. |
| 2 | Program the output type as 1, 2, or 3. |
| 3 | For type 1, program the ECP address and relay #. |
| 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 #93 Menu Mode Programming in the Programming Guide for a detailed explanation.*

# External Sounders

### In This Section



## General Information

The VISTA-128B 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 since the combined auxiliary power, polling loop, and alarm output in excess of 750mA must be supplied by the battery.

The output has the following options:

- Selectable for supervision
- Selectable for confirmation of arming ding (1-2 sec. sounding to confirm system has armed)
- 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.

## Alarm Output Supervision

When supervision is enabled, the panel monitors the alarm output wiring for open and short circuit faults while the output is inactive. The VISTA-128B will provide a trouble indication (Zone 970) when there is an open circuit in the alarm output wiring **that disconnects all indicating devices from the panel**, or when there is a short circuit between the Bell (+) and Bell (-) terminal wiring, (or between the Bell (+) terminal wiring and earth ground provided that the panel's earth ground terminal #30 is connected to a proper earth ground).

The VISTA-128B will indicate a trouble condition regardless of whether the system is armed or disarmed. The supervisory zone will display on the keypads, report to the event log, and transmit to the central station (if programmed), on Partition 1. The Contact ID event code is 321, Bell Trouble.

To use the supervision feature, do the following:

- Wire polarized fire-indicating devices to the alarm output as shown in *Figure 15-1*.
- Wire nonpolarized burglary indicating devices to the alarm output using a polarizing diode (two 2A diodes supplied), as shown in *Figure 15-2*.
- Program Zone 970 with a response type of 05 (trouble by day/alarm by night). See *Zone Programming* in the *#93 Menu Mode.*

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

If a device such as a siren driver with a high resistance trigger input (drawing less than 5mA) is being used, do the following:

- Cut the blue jumper on the upper left-hand corner of the panel's PC Board.
- Program Zone 970 with a response type of 00 (no response). See *Zone Programming* in the *#93 Menu Mode.*
- Mount the siren driver in the panel's cabinet.

**UL**

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

To disable the supervision feature, do the following:

- Cut the blue jumper on the upper left-hand corner of the panel's PC Board.
- Program Zone 970 with a response type of 00 (no response). See *Zone Programming* in the *#93 Menu Mode.*

## Installing Alarm Indicating Devices to the Alarm Output

Be sure to follow the proper guidelines below, depending on whether the system is installed in a UL or Non-UL application.

### Compatible Alarm Indicating Devices

**UL** Use only UL Listed sounding devices for UL installations

| Model Number | Device Type | Requires Polarizing Diode |
|---|---|---|
| **719** | Compact Outdoor Siren (not UL Listed) | Yes |
| **747** | Indoor Siren | Yes |
| **AB12** | Grade A Bell | Yes |
| **System Sensor MA 12/24D** | Fire Piezo Horn | No |
| **System Sensor P12575** | Fire Horn/Strobe | No |
| **Wheelock AS-121575W** | Fire Horn/Strobe | No |

### UL985 Household Fire or Combination Household Fire/Burglary Installations

For installations, which must provide UL Listed protection, the total current drawn from the alarm output, auxiliary power output, and polling loop combined, must not exceed 750mA in order to comply with the battery independence requirements. If, for example, two System Sensor PA400 piezo alarm sounders, wired in parallel, are used (24mA total), then 726mA (750mA – 24mA) is available for auxiliary output and polling loop use.

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

Wire polarized fire-indicating devices to the alarm output as shown in *Figure 15-1*.

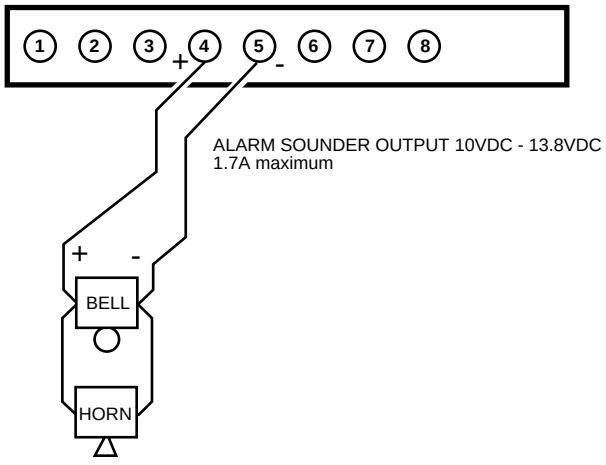



***Figure 15-1: Wiring Polarized Fire Indicating Devices***

### 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 since the combined auxiliary power, polling loop, and alarm output, in excess of 750mA must be supplied by the battery.

Wire nonpolarized burglary indicating devices to the alarm output using a polarizing diode as shown in *Figure 15-2*.

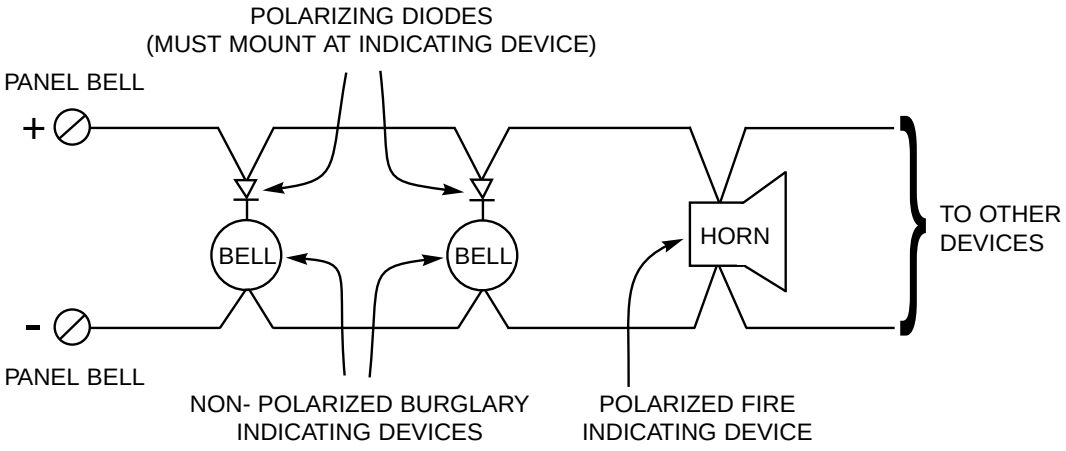



***Figure 15-2: Wiring Nonpolarized Burglary Indicating Devices***

### Non-UL Installations

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

### Programming the Alarm Output

Program the following data fields:

- ***13** Select Timeout for Bell
- ***16** Confirmation of Arming Ding for Bell
- ***21** PREVENT FIRE TIMEOUT (**1**=no timeout; **0**=fire timeout
- ***23** MULTIPLE ALARMS (partition-specific)
- **1*47** Enable Chime for Bell

# Event Log Options

### In This Section



## General Information

This system has the ability to record up to 512 events of various types in a history log. Each event is recorded in one of six categories with the time and date of its occurrence (if real-time clock is set). These categories are:

- Alarm
- Supervisory/check
- Bypass
- Open/close
- System conditions
- Test

The log may be viewed (Display Mode) on an alpha keypad, or can be printed (Print Mode) on a serial printer (connected to the system via a 4100SM Serial Interface Module).

## Event Log Printer Connections

The VISTA-128B's event log can be printed on a local serial printer.

Connect a UL EDP Listed serial printer to the J7 connector using an ADEMCO 4100SM Interface Module, as shown in *Figure 16-1*.

The 4100SM Module must be connected to the panel using the distance of the trigger cable. The wires ***cannot*** be lengthened to mount the module in a remote location.

The printer must be configured as follows:

- 7 data bits, even parity, 1 stop bit
- 300 or 1200 baud (1200 required if alpha numeric pager interface is installed)
- Hardware handshaking using DTR signal

The 4100SM Module is supplied with a 10-foot RS232 cable. A longer cable or an extension cable can be used if the VISTA-128B is separated from the serial printer by more than 10 feet, but the total cable length should be less than 50 feet.

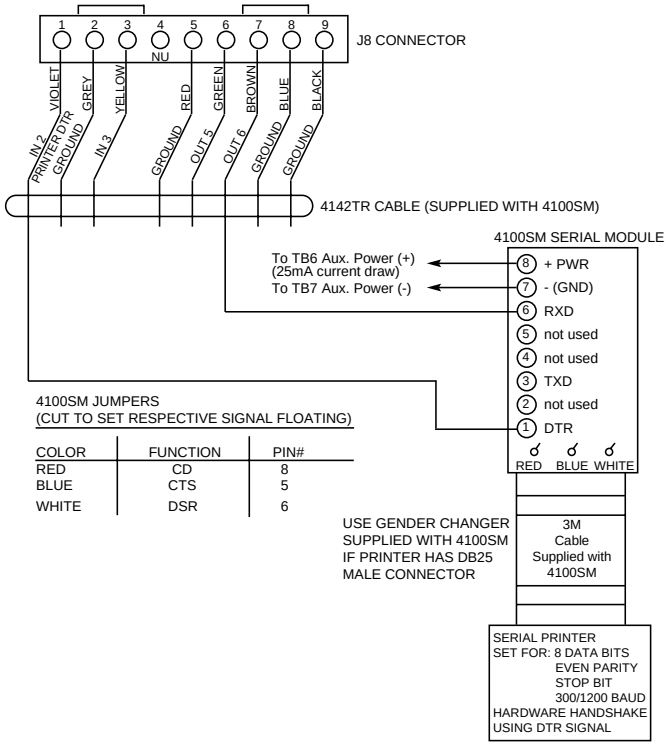



***Figure 16-1. Event Log Printer Connections***

Most printers either ignore the CTS, DSR, and CD signals, or require them to be high (i.e., 3-15VDC as measured on RS232 DB25 Connector Pins 5, 6 & 8, respectively, with respect to Ground Pin 7). The 4100SM Module sets these pins high. If the printer being used will not operate with these pins high, then clip the blue (CTS), white (DSR), or red (CD) jumpers on the 4100SM Module to set the corresponding signal floating. Important pins on the RS232C cable are Pin 3 (data out), Pin 7 (ground) and Pin 20 (DTR - ready).

The DTR signal, as measured at 4100SM TB1, should be high (9.5-14VDC) when the printer is powered, properly connected, on-line and ready to print. This signal will be low (0-1.5VDC) when the printer is not powered, not properly connected, off-line or out of paper. The VISTA-128B will not send printing data to the printer unless the DTR signal is high.

## Programming Event Log Options

Program the following data fields:

**1*70** EVENT LOG TYPES (**1**=enable; **0**=disable for each type)

**1*71** 12/24 HOUR TIME STAMP FORMAT (**0**=12 hr; **1**=24 hr)

**1*72** EVENT LOG PRINTER ON-LINE (**0**=disable; **1**=enable)

**1*73** PRINTER BAUD RATE (**1**=300; **0**=1200)

Enter *Report Code Programming* in the *#93 Menu Mode* to program report codes for the event log (System Group #4 codes).

If you need more information about actual programming procedures, see *The Mechanics of Programming* section.

## Event Logging Procedures

In order for proper time and date stamping to occur, the system's real-time clock must be set. Refer to the *Setting the Real Time Clock* section.

If you have selected the printer to be "on-line" (field 1*72), events will print automatically, as they occur. To display or print on demand, the following commands apply:

| **Commands** | |
|---|---|
| **Display Mode:** | Installer or Master Code + [#] + [6] + [0] |
| **Print Mode:** | Installer or Master Code + [#] + [6] + [1] |
| **Clear Event Log:** | Installer or Master Code + [#] + [6] + [2] |
| **To EXIT Event Log:** | Press [*] at any time. |

**Display/Printing:** After entering either the Display or Print Mode, the following will be displayed:

| |
|---|
| ENTER 0 = RECENT<br>1 = COMPLETE |

The event log holds up to 512 events, and can display or print all events in a category (complete), or only those events in a category occurring since the last "Clear Event Log" command (recent). Note that once the event log is full, the oldest event will be erased upon the logging of any new event. Press the desired Display Mode key, 0 or 1.

| |
|---|
| SCAN LOG BY PART<br>0=NO 1-8=PART # |

The system allows viewing of any partition's event log. Enter the partition number for the partition whose events are to be displayed. Entering 0 (NO) will display all events that occurred in the system, regardless of partition. Events are displayed in chronological order, from most recent to oldest.

For display and printing purposes, events are stored on a partition-by-partition basis (except system events), and are grouped into five categories, as follows.

**Use the [3] & [1] keys to scroll** to the next and previous screens, respectively:

| |
|---|
| ALARM EVENT LOG<br>TYPE CCC UUU |

Displays time/date for zones that have either caused an alarm or have been restored in selected partition.

| |
|---|
| CHECK EVENT LOG<br>TYPE CCC UUU |

Displays time/date for zones that have caused a trouble or supervisory condition in selected partition.

| |
|---|
| BYPASS EVENT LOG<br>TYPE CCC UUU |

Displays time/date for zones that have been bypassed in selected partition.

| |
|---|
| OP/CL EVENT LOG<br>TYPE CCC UUU |

Displays time/date and user number for each arming and disarming of the system for the partition selected.

| |
|---|
| SYSTEM EVENT LOG<br>TYPE CCC UUU |

Displays time/date for system problems, such as AC loss, communication failure, etc., regardless of partition.

| |
|---|
| ALL EVENT LOG<br>TYPE CCC UUU |

Displays all categories of events in chronological order, from most recent to the oldest.

| |
|---|
| TEST EVENT LOG<br>TYPE CCC UUU |

Displays all test events.

**To display the events in a particular category, press [8]** at the desired category screen.

If in Display Mode, the most recent event is displayed. Press [1] to display older events; press [3] to go forward in time.

If in Print Mode, the first press of [8] will cause the printer to print all events in that category, with each event automatically scrolled on the display keypad. The following is a typical display:

| |
|---|
| P8 01/01 12:02A<br>BURGLARY 003 |

Shows burglary alarm occurred in zone 3 of Partition 8, at 12:02AM on January 1.

After the last event in the selected category has been displayed (using either the [1] or [3] keys), the following will appear for a few seconds:

| |
|---|
| END OF EVENT LOG<br>TYPE CCC UUU |

| |
|---|
| CLEAR EVENT LOG<br>0=NO 1=YES |

Press [1] if Event Log Clear function is to be performed. Clearing the event log does not erase any events from the system memory. All events in the log will still be displayed if the COMPLETE option is selected. Only those events occurring from the time of the CLEAR command will be displayed if RECENT display option is selected. Press [0] if event log is **not** to be cleared at this time.

If [1] is pressed, the following will appear:

| |
|---|
| ARE YOU SURE?<br>0=NO 1=YES |

Press [1] if it is desired to clear the event log. Press [0] if event log is not to be cleared.

**SCREEN DEFINITIONS**

| | |
|---|---|
| **RECENT** | Events since last CLEAR |
| **COMPLETE** | Displays all events |
| **TYPE** | Type of event (burglary, fire, etc.) |
| **CCC** | Zone (contact) number |
| **UUU** | User number |

# 4100APG Pager Interface

### In This Section



## General Information

The VISTA-128B supports sending messages to a pager using the 4100APG Pager Interface. The 4100APG transmit to the pager any message programmed to be sent to the event log printer, even if the printer is not being used.

The types of messages are divided into 6 categories: Alarms; Troubles; Bypasses; Openings/Closings; System and Test. Each type has its own programming field for the pager phone number and pager ID. This allows each message either to be sent to a different paging service or to the same service.

The 4100APG will hang up between each message. Multiple messages will be sent in the order received. If the 4100APG cannot make contact with the paging service, it will retry up to 10 times. If the interface loses contact with the VISTA-128B, it will send a message to the paging service to notify the user.

The pager interface must be wired to a different phone line than the VISTA-128B itself. Otherwise, the communication of both will not function properly.

## Mounting the 4100APG

The 4100APG may be mounted either inside or outside the control cabinet.

Do not mount the 4100APG on the cabinet door or attempt to attach it to the PC board.

To mount the 4100APG, perform the following steps:

| Step | Action |
|---|---|
| 1 | **If you are mounting the 4100APG inside the control cabinet**, attach it to the cabinet's interior surface with 2-faced adhesive tape. You may leave the interface's cover off. |
| 2 | **If you are mounting the 4100APG outside the cabinet**, use the screw holes at the rear to mount horizontally or vertically (2-faced adhesive tape may be used, if preferred). You can bring wires out from the side or back (a round breakout is also available on the back). |

## Wiring the 4100APG

The 4100APG may be used either with or without a serial printer. The 4100APG connects to the VISTA-128B via the 4100SM. The 4100SM connects to the J8 connector on the control via the 4142TR Cable.

### Without the Event Log Printer

#### Connecting the 4100SM to the Control:

To connect the 4100SM to the control, perform the following steps:

| Step | Action |
|---|---|
| 1 | Connect the 4142TR to J8 on the control. See *figure 17-1*. |
| 2 | Connect the RED wire of 4142TR to TB1-6 of 4100SM (RxD). |
| 3 | Connect the VIOLET wire of 4142TR to TB1-1 of 4100SM (DTR). |
| 4 | Connect TB1-7 of 4100SM to terminal 7 (Auxiliary Power -) of the control. |
| 5 | Connect TB1-8 of 4100SM to terminal 6 (Auxiliary Power +) of the control |

#### Connecting the 4100APG to the 4100SM

To connect the 4100APG to the 4100SM, perform the following steps:

| Step | Action |
|---|---|
| 1 | Connect the Incoming telephone line to the 4100APG RJ11 connector labeled LINE. See *figure 17-1*. |
| 2 | (Optional) Connect the Handset side of telephone line to 4100APG RJ11 connector labeled PHONE. |
| 3 | Connect the DB25M to DB-9M Cable (supplied), from 4100SM (25 pin) to 4100APG (9 pin) connector labeled SERIAL PORT INPUT. |

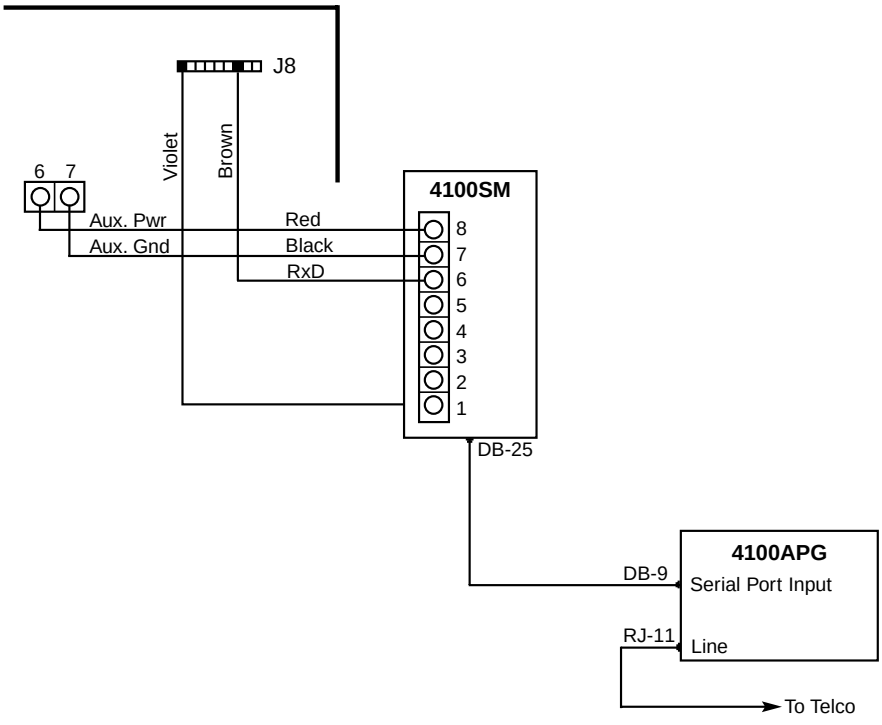



***Figure 17-1: Wiring the 4100APG Without the Serial Printer***

### With the Event Log Printer

The serial printer must be configured for 1200 baud rate, seven data bits, even parity, and one stop bit. **(7/E/1).**

To connect the 4100APG with a serial printer, perform the following steps:

| Step | Action |
|---|---|
| 1 | Perform the steps outlined for connecting 4100APG Without a Serial Printer. |
| 2 | Connect a DB-25 to DB-25 cable from the printer to the 4100SM. See *figure 17-2.* |
| 3 | Configure the printer for 1200 baud rate, seven data bits, even parity, and one stop bit. **(7/E/1).** |

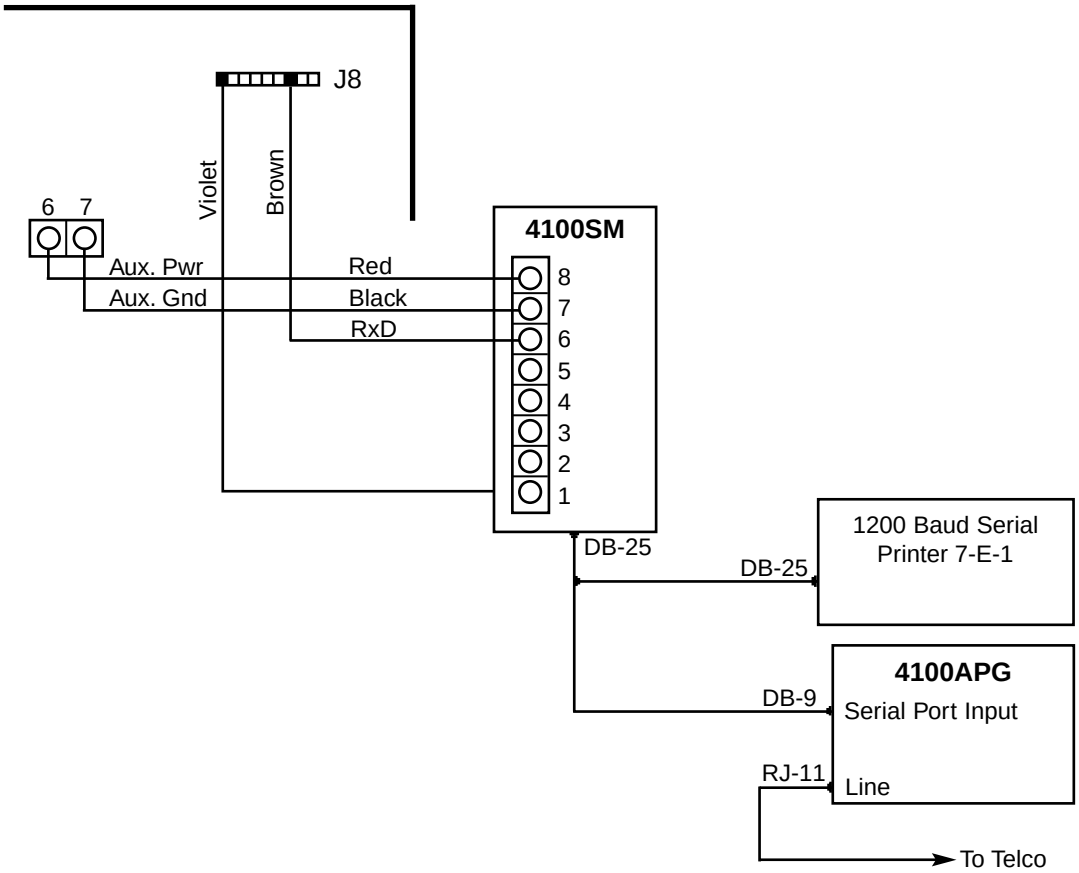



***Figure 17-2: Wiring the 4100APG With the Serial Printer***

When you complete the module's mounting and wiring, you should install the module's cover (with label affixed).

## Programming the Control for the Pager

- In field *64 enter **1** to enable the 4100APG pager interface.
- In field *65 enter the phone number of the paging service for Alarm reports. Up to 17 digits may be entered.
- In field *66 enter the Pager ID number of the paging service for Alarm reports. This is the PIN number. Up to 10 digits may be entered.
- In field *67 enter the phone number of the paging service for Trouble reports. Up to 17 digits may be entered.
- In field *68 enter the Pager ID number of the paging service for Trouble reports. This is the PIN number. Up to 10 digits may be entered.
- In field *69 enter the phone number of the paging service for Bypass reports. Up to 17 digits may be entered.
- In field *70 enter the Pager ID number of the paging service for Bypass reports. This is the PIN number. Up to 10 digits may be entered.
- In field *71 enter the phone number of the paging service for Open/Close reports. Up to 17 digits may be entered.
- In field *72 enter the Pager ID number of the paging service for Open/Close reports. This is the PIN number. Up to 10 digits may be entered.
- In field *73 enter the phone number of the paging service for System reports. Up to 17 digits may be entered.
- In field *74 enter the Pager ID number of the paging service for System reports. This is the PIN number. Up to 10 digits may be entered.
- In field *75 enter the phone number of the paging service for Test reports. Up to 17 digits may be entered.
- In field *76 enter the Pager ID number of the paging service for Test reports. This is the PIN number. Up to 10 digits may be entered.
- In field 1*70 enable the events for the event log.
- In field 1*72 enable the **Printer On-Line** option. This must be turned on to allow events to be sent to the pager interface when they occur.

## 4100APG LED Indications

Below is a table outlining the LED indications:

| LED Name | Steady | Blinking | Off | Pulse |
|---|---|---|---|---|
| **Power** | OK | On Battery (B/U) | No Power | |
| **Line** | Not in use (OK) | | In Use | |
| **Call** | Call in Progress | Page Retry | Idle | |
| **Busy** | Telephone Busy | No Dial Tone | OK | |
| **Page** | | Page Fail | OK | Page OK |
| **Data** | | | No Data | Msg Data |
| **Load** | | | No Data | Prog Data |
| **TRBL** | | Trouble | OK | |

# Final Power-Up Procedure

## In This Section



## General Information

- You can power the control from the supplied 1361 Transformer (1361CN in Canada), rated 16.5VAC, 40VA, which plugs directly into a 24 hour, 120VAC, 60 Hz outlet.
- If you are using powerline carrier devices, you must use the 4300 Transformer instead.

---

**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 in order 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 combined the auxiliary power, the polling loop and the alarm output current in excess of 750mA.

## Earth Ground Considerations

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. We recommend using #16 AWG copper wire run at a maximum length of 25 ft. The following are examples of good earth grounds available at most installations:

- **Metal Cold Water Pipe:** Use a non-corrosive 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.

## Connecting the Transformer

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.

| Step | Action |
|---|---|
| 1 | Use the Polling Loop Current Draw and Auxiliary Device Current Draw Worksheets found later in this section to make sure that the currents drawn by the devices connected to the system do not exceed the system's respective ratings. |
| 2 | Connect all installed devices to the control. |
| 3 | Wire the 1361 Transformer (1361CN in Canada) to the panel (before connecting the battery) as shown in *Figure 18-1*, or wire the 4300 Transformer as shown in *Figure 18-2* (if using Powerline Carrier devices). |
| 4 | Plug the transformer into a 24 hour, uninterrupted, 120VAC, 60Hz outlet. After a few seconds, the keypad display will appear. |

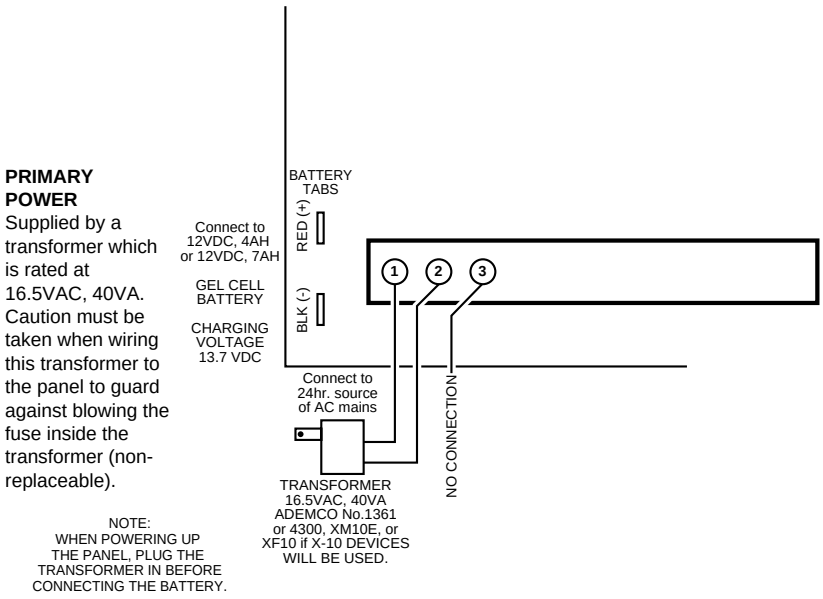



***Figure 18-1: 1321 Transformer and Battery Connections***

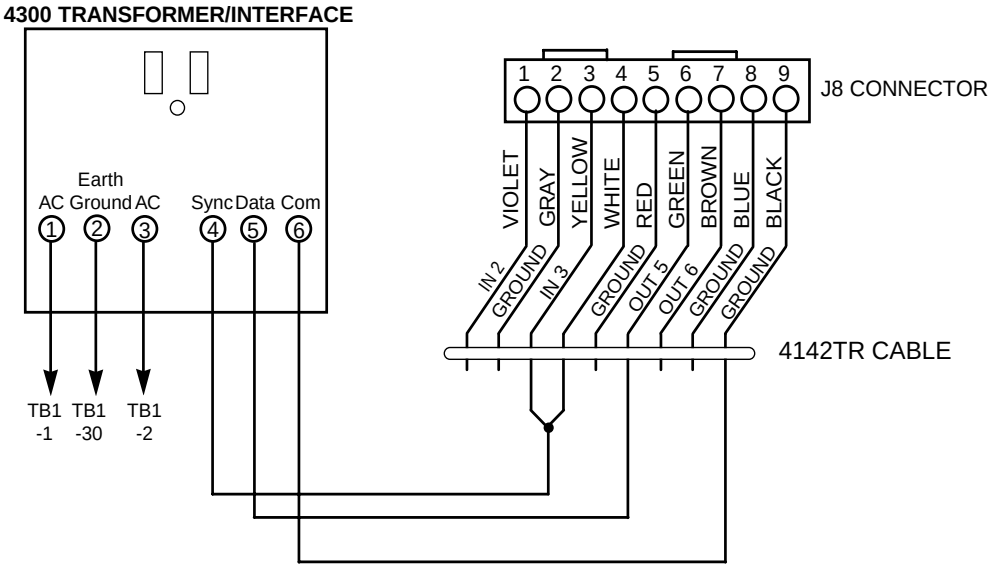



***Figure 18-2: 4300 Transformer Connections***

## Programming Power and AC Options

Program the following data fields:

***17** AC POWER LOSS KEYPAD SOUNDING (**1**=yes; **0**=no)

***19** AC RANDOMIZE (1=randomize; 0=no)

***28** POWER UP IN PREVIOUS STATE (**1**=yes; **0**=no)

If you need more information about actual programming procedures, see *The Mechanics of Programming* section.

## Determining the Control Panel Power Supply Load

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

### 1. Table 1: Total Polling Loop Current Draw

Refer to the instruction accompanying the device for the current draw. Refer to the POLLING LOOP section for device restrictions for fire and burglary usage.

| Polling Loop | 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. This module is powered from the panel's auxiliary power, and provides a separate polling loop output, which can support an additional 128mA load. 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**

| | | | Total Current | |
|---|---|---|---|---|
| **Device Model #** | **Device Current X** | **# of Units =** | **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**

| | | | Total Current | |
|---|---|---|---|---|
| **Device Model #** | **Device Current X** | **# of Units =** | **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-128B Current Load**

| | Total Current | |
|---|---|---|
| | **Standby** | **Alarm** |
| Polling Loop Subtotal (see Table 1) | | |
| Auxiliary Power Subtotal (see Table 2) | | |
| Alarm Output Subtotal (see Table 3) | | |
| VISTA-128B PCB Current (Includes 2-wire smoke detector loading on zones 1 & 2) | 250mA | 330mA |
| **Total Current Load** | | |

## Determining the Size of the Standby Battery

The cabinet supplied with the VISTA-128B panel can house up to 12V, 14AH batteries (two 12V, 7AH batteries wired in parallel). The VISTA-ULKT kit provides a cabinet that can house up to 12V, 17.2AH batteries 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 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**

Household Fire or Combination Household/Fire/Burglary installations require the use of a backup battery that is capable of proving 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 6 to determine the required backup battery capacity and use Table 7 to determine the battery model number. **A dual battery harness is supplied** that allows two batteries to be wired in parallel for increased capacity.

### Battery Capacity Calculation Table

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

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

### Battery Selection Table

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

| 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 will cause a battery test to be initiated. The VISTA-128B will also run a 5-second battery test every 60 seconds to check if the battery is connected

# The Mechanics of Programming

### In This Section



## Using Data Field Program Mode

Data Field Program Mode is the program Mode whereby many system options are programmed. The field numbers on the program form show the number of entries required for each field. When an entry is completed, the keypad beeps three times and advances to the next field. At this point, you can either make the required entry in the new field, or press [∗] + the next field number you want to program.

There are several "question and answer" modes, which we call "Menu" Modes, that can be accessed once Data Field Program Mode has been entered. These modes prompt the user for information, and for this reason, a 2-line alpha keypad (6139) is required.

The factory-loaded defaults (*97) enable keypad addresses 00-03 only. A keypad set to one of these addresses must be used to program the system.

## Entering Data Field Programming Mode

Enter Program 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.**

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

## Moving from One Page of Programming to Another

The data fields are grouped into four 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. The words "ALT PROGRAM MODE" is displayed along with a "100, or "200," depending on which page of program fields is accessed, to indicate the higher page of fields.

1. To access the next level of fields, press ∗94.
2. Then press [✳] + [XX], where XX = the last two digits of the program field, and make the desired entry.
3. To return to the previous page of fields, press ∗99.

**Press *94 to move to 2nd page; press *99 to move back to 1st page**

| second page of fields (1*01-1*76) |
|---|

**Press *94 to move to 3rd page; press *99 to move back to 2nd page**

| third page of fields (2*00-2*24) |
|---|

## Viewing Data Fields

To view the contents of a data field, press [#] plus the 2-digit field address. The field's entries will be displayed, but no changes can be made.

## Entry Errors

- If an address is improperly entered, the keypad will display “FC”.
- If a program entry is improperly entered (for example, a larger number than that which is permitted), the keypad display will go blank.
- In either of the above cases, simply re-enter [✳] + the correct field number.

| SUMMARY OF DATA FIELD PROGRAMMING COMMANDS | |
|---|---|
| ***91** | Select partition for programming partition-specific fields |
| ***92** | Will display the software revision level of the control panel |
| ***93** | Enters 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 |

## Programming System-Wide Data Fields

Values for some programming fields are system-wide (global), and some can be different for each partition (partition-specific). Note that the partition-specific programming fields are automatically skipped when programming the global fields. If the system has only 1 partition, the partition-specific fields *will not* be automatically skipped.

To program system-wide data fields, do the following:

| Step | Action |
|---|---|
| 1 | Enter Program Mode: **[Installer Code] + 8 0 0 0.**<br>After entry into the Program Mode, the following will be displayed:<br>Program Mode<br>*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, Installer's Code). Make the desired entry. When the field is complete, the keypad will beep three times and will advance to the next field. If you do not desire to change the next field, press [✳] and enter the next field number to be programmed.<br>First Page of fields<br>(*00-*90) |
| 4 | To change to the next page of fields, press ***94**. To return to the previous page of fields, press ***99**. |
| 5 | **Press *99 or *98 to exit Program Mode** |

- If the number of digits that you enter in a data field is less 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 (e.g., press ∗08).
- Partition-Specific Programming Fields are skipped unless entered specifically.

## 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.**<br>After entry into the Program Mode, the following will be displayed:<br>Program Mode<br>*Fill # View -00 |
| 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 will automatically be displayed. When all partition-specific fields are programmed, the system returns to the global programming fields (page 1 fields). To return to the global program fields before finishing all fields, enter any global field number. |
| 4 | Repeat this procedure for each partition in the installation. |

**PROGRAMMING PARTITION-SPECIFIC FIELDS**

**Press *91 to select a partition.**

↓

**Enter the partition to be programmed.**

↓

**Enter a partition-specific field # 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 a mode through which much of the system's programming is done. It offers main menu selections for the following:

- Zone Programming
- Expert Mode Programming
- Report Code Programming
- Alpha Programming
- Device Programming
- Output Programming
- Relay Voice Descriptors
- Custom Index Programming (VIP Module substitute words)
- Access Point Programming (used for VistaKey modules)
- Access Group Programming (used for VistaKey modules)
- Event/Action Programming (used for VistaKey modules)

Press 0 (NO) or 1 (YES) in response to the displayed menu selection. Pressing 0 will display the next choice in sequence. The keypad will then prompt you with questions regarding the programming of a particular zone or device. (Refer to the individual sections to program each option shown.)

The following is a list of commands used while in the Menu Mode.

**#93 Menu Mode Key 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+ [✳] | Escapes from Menu Mode, back into Data Field Programming Mode, if entered at the first prompt of each main menu option. |

# Zone Type Definitions

### In This Section



## Zone Number Designations

The VISTA-128B supports up to 128 zones of hardwire, polling loop and/or wireless protection, distributed among up to 8 partitions. The following table lists the zone numbers and the types of sensors that can be used with each in this system, and some alternate functions the zones may be used as:

| Zone | Sensors |
|---|---|
| 1 | 2-wire Smoke Detectors (if used) |
| 5 | Audio Alarm Verification (if used) |
| 7 | Keyswitch (if used) |
| 8 | Latching-Type Glassbreak Detectors (if used) |
| 1-9 | Traditional Hardwired Zones |
| 9 | Programmable for Fast Response |
| 1-128 | 5800 Series Wireless Devices |
| 10-128 | Polling Loop Devices |
| 995 | ✳ + 1 Panic |
| 996 | # + 3 Panic |
| 999 | ✳ + # Panic |

## Zone Type Definitions

Each zone must be assigned a zone type, which defines the way in which the system responds to faults in that zone. In addition, 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 a zone 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 the primary entry and exit of the facility.

### Type 02: Entry/Exit #2 Burglary

Provides a secondary entry delay whenever the zone is faulted and the system is armed in the AWAY and STAY mode. 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 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 zones of exterior doors and windows.

### 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.

**Interior Follower zones are 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/exit time), if tripped when the panel is armed in the AWAY mode and exit delay only when armed in MAXIMUM mode. **Interior with Delay zones are 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 20: Arm-STAY✳**

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

**Type 21: Arm-AWAY✳**

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

**Type 22: Disarm✳**

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**

Indicates that an input device (hardwired zone, wireless zone, keypad, access control relay, etc.) is controlling an access point entry (e.g., a door). The access point entry relay can be assigned to an access control relay (controlled by the VISTA-128B), ECP relay (4204), or to the access control system independent of the VISTA-128B.

**Type 28: Main Logic Board (MLB) Supervision**

Used to supervise the MLB. If communication between the MLB and the Vista Gateway Module (VGM) fails, a trouble condition is annunciated for the zone. Also, if the communication fails, all access control system (ACS) input zones will also display a "CHECK."

**Type 29 Momentary on 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 back to an entry point. This zone type should be only used with VistaKey modules.

✳ Note that these zone types are for use by 5800 Series devices *only!*

**NOTE FOR PANIC KEYS:** Keypad panic zones share the same zone response type for all 8 partitions, but panics may be individually enabled for each partition.

**IMPORTANT! FAULT ANNUNCIATION**

Polling loop and RF troubles (zones 988, 990 & 997) will report as trouble conditions only, and as such, should be assigned zone type 05 if annunciation is desired. See *Polling Loop Supervision* in the *2-Wire Polling Loop Expansion* section and *RF System Operation and Supervision* in the *Wireless Expansion* section for more information.

# Zone Index/Zone Type Defaults

### In This Section



## Zone Index

The VISTA-128B has 128 protection zones, as well as supervisory zones for relays, ECP devices (devices which communicate through the keypad terminals), and system troubles. These zones are designated as follows:

| ZONE # RANGE | ZONE FUNCTION | ACTUAL ZONE |
|---|---|---|
| 001 - 128 | Protection zones | As indicated |
| 601 - 632 | Relay Supervisory Zones | 6 + 2-digit Relay Number; e.g., Relay Number 03, if supervised, is zone 603. |
| 800 - 830 | ECP Device Supervisory Zones (includes keypads, wireless receivers, VIP Module, relay modules, etc.) | 8 + 2-digit Device Address; e.g., Device Address 01, if supervised, is zone 801. The 4285/4286 VIP Module is zone 804 (since its Device Address must be set to 4). |
| 970, 988,-990, & 997 | System Supervisory Zones | 970: Bell Supervision<br>988: 2nd Wireless Receiver - not receiving signals<br>990: 1st Wireless Receiver - not receiving signals<br>997: Polling Loop (short circuit) |
| 995 - 999 | Keypad Panics | 995: 1 + ∗ panic (A key)<br>996: 3 + # panic (C key)<br>999: ∗ + # panic (B key) |

Response types for zones are enabled in *Zone Programming* in the *#93 Menu Mode.* Supervisory zones should be given a response type of 05 (Trouble by Day, Alarm by Night).

## Zone Type Defaults

Following are the zone type defaults for zones on the VISTA-128B:

| Zone # | Zone Type |
|---|---|
| 001 | 09 |
| 002 | 03 |
| 003 | 03 |
| 004 | 03 |
| 005 | 03 |
| 006 | 03 |
| 007 | 03 |
| 008 | 03 |
| 009 | 03 |

| Zone # | Zone Type |
|---|---|
| 010–128 | 00 |
| 601-632 | 05 |
| 800-830 | 00 |
| 970 | 00 |
| 988 | 00 |
| 990 | 00 |
| 995 | 00 |
| 996 | 00 |
| 997 | 05 |
| 999 | 06 |

# Data Field Descriptions

The following is a description of all data fields provided by this control. If you have followed earlier instructions during the installation of the various devices, some of these fields may already have been programmed.

If you need more information about actual programming procedures, see *The Mechanics of Programming* section.

***00 INSTALLER CODE** [4140] | | | |

The Installer's 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 not used to arm the system. This code cannot reenter Programming Mode if exited by the *98 command.

***09 ENTRY DELAY #1 (partition-specific)** [02] |

Entry delay defines the delay time which 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. Enter the entry delay time (**01-15** multiplied by 15 seconds, or **00** for no delay), up to a maximum delay of 225 seconds (entry **15** multiplied by 15 seconds), for zones assigned to Zone Type 01.

***10 EXIT DELAY #1 (partition-specific)** [03] |

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. Enter the exit delay time (**01-15** multiplied by 15 seconds or **00** for no delay), up to a maximum delay of 225 seconds, for zones assigned to Zone Type 01.

***11 ENTRY DELAY #2 (partition-specific)** [06] |

Entry Delay #2 is used for a secondary door requiring a longer delay than those assigned to Entry Delay #1. This delay may not exceed 45 seconds for UL commercial burglary installations.

***12 EXIT DELAY #2 (partition-specific)** [08] |

Exit Delay #2 is used for a secondary door requiring a longer delay than those assigned to Exit Delay #1. This delay may not exceed 60 seconds for UL commercial burglary installations.

***13 BELL TIMEOUT (partition-specific)** [04] |

Defines the length of time Bell Output 1 and the keypad's sounder will sound for all audible alarms (multiply entry 01-15 by 2 minutes for actual duration).

Must be a minimum of 16 minutes for UL commercial burglary installations.

***14 ZONE 9 RESPONSE TIME** [0]

Enter **1** to set fast response mode (10 msec) for appropriate devices wired to zone 9. Enter **0** for normal response (350 msec). Must be **0** for UL.

***15 KEYSWITCH ASSIGNMENT** [0]

Enter the partition number **1-8** in which the keyswitch is being used. Otherwise, enter **0.**

Requires the use of zone 7 wired loop (zone 7 is no longer available as protection zone when used for keyswitch operation). If the keyswitch is used, the fire and panic alarm voltage triggers automatically become ARMING and READY status outputs for support of the Keyswitch LEDs.

Reports openings/closing by user "0" if reporting is enabled in field *40.

***16 CONFIRMATION OF ARMING DING (part.-specific)** [0]

Enter **1** to enable 1/2 second external alarm sounding ("ding") at the end of exit delay (or after kissoff from the central station, if sending closing reports). Otherwise enter **0**. Must be 1 for UL commercial burglary installations. Bell test on arming is required in UL commercial burglary installations.

***17 AC LOSS KEYPAD SOUNDING** [0]

Enter **1** to enable sounding at the keypad (rapid beeping) when AC power is lost (sounding occurs about 2 minutes after actual AC loss).

Enter **0** if no AC power loss keypad sounding is desired.

***19 RANDOMIZE AC LOSS REPORT** [0]

Selecting this option helps prevent an overload of AC loss messages at the central station during a community blackout.

Enter **1** to randomize AC loss reporting between 10 and 40 min. after an actual AC loss. Enter **2** for 6-12 hours after AC loss. Enter **0** for normal AC loss reporting (about 2 minutes after actual AC loss).

***20 VIP MODULE PHONE CODE** [00, 11]

If a 4285/4286 Voice Module is being used, enter the 2-digit phone code used to access the system.

Enter **01-09** for first digit, and enter **11** (for ✳) or **12** (for #) for second digit.

To disable the voice module, enter **00** for the 1st digit and enter **11** for the 2nd digit of the code (disable code = 00,11). Must be disabled for commercial fire and UL commercial burglary installations.

***21 PREVENT FIRE TIMEOUT** [0]

Enter **1** to disable (no timeout) the alarm sounder duration for any zone designated as a fire zone, regardless of partition, so that fire sounding continues until the system is reset.

Enter **0** if the normal burglary sounder duration (programmed in partition-specific field *13) should apply to fire alarms.

***22 KEYPAD PANIC ENABLES (partition-specific)** [001]

95 96 99

Enter **1** to enable the appropriate keypad panics used in this partition.

Otherwise enter **0**.

***23 MULTIPLE ALARMS (partition-specific)** [1] ☐

Determines whether or not more than one alarm can be sounded in 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 selection applies to local sounding and has no impact on the number of communication messages transmitted. Refer to ∗84 Swinger Suppression for limiting communication messages. Enter **1** if this feature is desired. Enter **0** if not desired. Must be 1 for UL installations.

***24 IGNORE EXPANSION ZONE TAMPER** [0] ☐

Enter **1** to disable (ignore) tamper.

Enter **0** if tamper detection is desired. Must be **0** for UL installations.

**Note:** Only applicable to certain polling loop sensors with tamper switches or 5800 Series transmitters. This option is used to disable tamper detection on these devices.

***25 BURG. TRIGGER FOR RESPONSE TYPE 8** [1] ☐

Enter **1** to allow optional triggering of the voltage output on Pin 3 of the J2 header to include zone response type 8 (24-hr. auxiliary).

Enter **0** if only burglary and audible panic alarms (zone type 7) will trigger Pin 3.

***26 INTELLIGENT TEST REPORTING** [0] ☐

Enter **1** if no test report is to be sent if any other type of report was sent since the last test report.

Enter **0** if test reports are to be sent at the set intervals, regardless of whether or not other reports have been sent. Must be **0** for UL applications.

***27 TEST REPORT INTERVAL** [024] | |

Enter the test reporting interval in hours, **001-999.**

Enter **000** if no test reporting is desired. If a test report is desired, enter a test code in *Report Code Programming* in the *#93 Menu Mode.*

Set first test report time in field *83.

Max. 024 for UL commercial burglary installations.

***28 POWER UP IN PREVIOUS STATE** [1] ☐

Enter **1** if upon power-up, after a prolonged power loss which caused the system's battery to discharge, the system will assume the system status prior to the power loss.

Enter **0** if the system is always to power up in a disarmed state. When the system powers up armed, an alarm will occur 3 minutes after arming if a zone is faulted. When so armed, the system reports closing as User #0 if Open/Close reporting for installer was enabled in field *39. Note that if the previous state was armed AWAY or STAY, the system may not respond to sensor changes for a small period of time (1-3 min.), which allows sensors such as PIRs to stabilize.

**Note:** Must be **1** for UL applications. Note that authority levels 0 or 5 cannot be used to disarm the system if the control powers up armed.

***29 QUICK ARM (partition-specific)** [1] ☐

Enter **1** to enable arming of the burglary system in AWAY, STAY, INSTANT or MAXIMUM modes by using the # key instead of the user code. 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. Enter **0** if Quick Arm is not desired. (The user code must always be used to disarm the system.) Note that if Quick Arm is used, the Installer Code and Authority Level 5 codes cannot disarm the system.

***30 TOUCHTONE OR ROTARY DIAL** [0] ☐

Enter **1** if TouchTone service is being used.

Enter **0** if rotary phone service is used.

If selecting TouchTone, make sure the subscriber has requested and is paying for TouchTone service. Note that whether or not TouchTone dialing for call placement is permitted, communication by the use of DTMF signaling (ADEMCO High Speed) will still take place. See field 1*33 for TouchTone w/Rotary backup.

***31 PABX ACCESS CODE** | | | |

This field is used to enter up to four 2-digit numbers 00-09; B-F (11-15). If not required, enter nothing and proceed to next address; otherwise, enter prefix needed to obtain an outside telco line.

***32 PRIMARY SUBSCRIBER ACCT # (partition-specific)** | | | |

Enter 00-09; B-F (11-15) [15 15 15 15]

Enter a 3-or 4-digit (depending on report format) primary subscriber account number 00-09; B-F (11-15). Each number requires a 2-digit entry so as to allow entry of hexadecimal digits (B-F). If a 3-digit account number is to be used, enter data only in the first 3 locations, leaving the last one unfilled, by entering a *.

***33 PRIMARY PHONE NUMBER** | | | | | | | | | | | | | | | |

This field is used to enter the primary central station phone number, up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** 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.

***34 SECONDARY PHONE NUMBER**

| | | | | | | | | | | | | | | | |

This field is used to enter the secondary phone number, up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** 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. If this field is programmed, a secondary subscriber account number (field *90) *must* also be programmed (can be the same as the primary account number).

***35 DOWNLOAD PHONE NUMBER**

| | | | | | | | | | | | | | | | |

This field is applicable only if downloading will be utilized.

Enter the downloading phone number, up to 17 digits, **0-9**; **enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces.

***36 DOWNLOAD ID NUMBER**

| | | | | | | | |

Enter eight digits, 00-09; A-F (10-15). Only applicable if downloading will be utilized. Make entries as 2-digit numbers as follows:

00=0 02=2 04=4 06=6 08=8 10=A 12=C 14=E

01=1 03=3 05=5 07=7 09=9 11=B 13=D 15=F

***37 DOWNLOAD COMMAND ENABLES**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Dialer Shutdown | System Shutdown | Not Used | Remote Bypass | Remote Disarm | Remote Arm | Upload Program | Download Program |

Each of the various remote functions can either be enabled or disabled through Compass downloading software. Disabling a function means that you will not be able to perform that function from Compass. Default values = [11011111].

Enter **1** to enable a function, enter **0** to disable. See field 1*53 to disable the download callback option. For UL commercial burglary installations, all entries must be **0**.

***38 PREVENT ZONE XXX BYPASS (partition-specific)** [000] | |

Entering a zone number **(001-128)** prevents that zone from being bypassed by the user.

Enter **000** if this feature is not desired (all zones can be bypassed).

***39 ENABLE OPEN/CLOSE REPORT FOR INSTALLER CODE(partition-specific)** [1] ☐

Enter **1** if Open/Close reporting for the installer is desired.

Otherwise enter **0**.

***40 OPEN/CLOSE REPORTING FOR KEYSWITCH** [0] ☐

Enter **1** to enable Open/Close reporting for the keyswitch.

Enter **0** if reporting is not desired.

***41 NORMALLY CLOSED OR EOLR (ZONES 2-8)** [0] ☐

Enter **0** if end-of-line resistors are to be used.

Enter **1** if end-of-line resistors are not to be used, in which case only **normally closed** devices must be used.

Must be **0** for UL installations.

***42 DIAL TONE PAUSE** [0] ☐

This field sets the time the system will wait for dial tone before dialing. Applies if true dial tone is not selected in field *43.

Enter the desired wait time for dial tone detection as follows: Enter single digit: **0** = 5 seconds; **1** = 11 seconds; or **2** = 30 seconds. Must be **0** for UL installations.

***43 DIAL TONE DETECTION** [1] ☐

Determines whether the control will wait for a true dial tone before dialing, or if it will wait for a predetermined delay before dialing (delay is programmed in Dial Tone Pause field *42). The latter may be necessary in high-noise environment telco networks where noise can be confused with dial tone, resulting in premature dialing.

Enter **1** for true dial tone wait. If no dial tone is detected, will dial at end of pause programmed in field *42.

Enter **0** to pause for seconds entered in field *42, then dial.

***44 RING DETECTION COUNT** [00] [ | ]

Only applicable if using a 4285/4286 VIP Module and/or if station-initiated downloading will be used.

Enter **00** to disable ring detection.

Enter **01-14** for ring counts of 1-14.

Enter **15** to select Answering Machine Defeat Mode, which allows the system to receive calls even when a telephone answering machine is connected to the same phone line. 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, will not answer the first call, but will ready 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 commercial burglary installations.

**Note:** Do not enter 00 if a 4285/4286 is installed.

***45 PRIMARY FORMAT** [0] [ ]

This field selects the reporting format for use on the primary telephone number.

Enter the appropriate number for the primary format as follows: **0**=Low Speed; **1**=Contact ID; **2**=ADEMCO High Speed; **3**=ADEMCO Express

***46 LOW SPEED FORMAT (PRIMARY)** [0] [ ]

Enter the appropriate value: **0**=ADEMCO Low Speed; **1**=Sescoa/Radionics

***47 SECONDARY FORMAT** [0] [ ]

This field selects the reporting format for the secondary telephone number.

Enter the appropriate number for the secondary format as follows: **0**=Low Speed; **1**=Contact ID; **2**=ADEMCO High Speed; **3**=ADEMCO Express

***48 LOW SPEED FORMAT (SECONDARY)** [0] [ ]

Enter the appropriate value: **0**=ADEMCO Low Speed; **1**=Sescoa/Radionics

***49 CHECKSUM VERIFICATION** [0,0] [ ] [ ]

Enter **1** for either or both primary/secondary formats to send a verification digit to validate the message at the receiver without having to send two message rounds. Selection is valid for 3+1, 4+1, and 4+2 reports.

Enter **0** if not desired.

***50 SESCOA/RADIONICS SELECT** [0] [ ]

Enter **0** if Radionics format is to be used with hexadecimal 0-9, B-F reporting. Enter **1** if Sescoa format is to be used with only numeric reporting (0-9). Note that selection applies to both primary and secondary phone numbers.

***51 DUAL REPORTING** [0] [ ]

This field allows all reports to be sent to both primary and secondary phone numbers.

Enter **1** if all reports are to be sent to both primary and secondary phone numbers. 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.

***52 STANDARD/EXPANDED REPORT PRIMARY**

| Alm | Rst | Byp | Trbl | Opn/Cls | Low Batt |
|---|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Enter **0** for standard or **1** for expanded reporting for the primary phone number; default is **0**.

**Note:** Expanded overrides 4+2 format.

***53 STANDARD/EXPANDED REPORT SECONDARY**

| Alm | Rst | Byp | Trbl | Opn/Cls | Low Batt |
|---|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Enter **0** for standard or **1** for expanded reporting for the secondary phone number; default is **0**.

**Note:** Expanded overrides 4+2 format.

***56 USE ONLY LRR (LONG RANGE RADIO)** [0] ☐

Enter **1** if the built-in dialer is not being used and only the LRR will be used to communicate. Otherwise enter **0**.

***57 USE LRR (LONG RANGE RADIO) IF DIALER FAILS** [0] ☐

Enter **1** if LRR is to be used as a backup to the built-in dialer if the dialer fails. The radio messages begin transmitting the same time as the dialer. Once the dialer receives a kissoff, the LRR will stop transmitting no matter where it might be within its sequence. Otherwise enter **0**.

***58 LONG RANGE RADIO CENTRAL STATION #1 CATEGORY ENABLE**

| Alm | Trbl | Byp | Opn/Cls | Syst | Test |
|---|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Enter **1** to enable reports for primary Subscriber ID of Long Range Radio. Otherwise, enter **0**. Default = 0.

***59 LONG RANGE RADIO CENTRAL STATION #2 CATEGORY ENABLE**

| Alm | Trbl | Byp | Opn/Cls | Syst | Test |
|---|---|---|---|---|---|
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Enter **1** to enable reports for secondary Subscriber ID of Long Range Radio. Otherwise, enter **0**. Default = 0.

***64 ALPHA NUMERIC PAGER INSTALLED** [0] ☐

Enter **1** if the alpha numeric pager interface is installed. Otherwise enter **0**.

***65 PAGER PHONE NUMBER FOR ALARMS**

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |

This field is used to enter the alpha numeric paging service phone number for Alarm reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***66 PAGER ID NUMBER FOR ALARMS**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

This field is used to enter the Pager ID number for Alarm reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***67 PAGER PHONE NUMBER FOR SUPERVISION**

This field is used to enter the alpha numeric paging service phone number for Trouble reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***68 PAGER ID NUMBER FOR SUPERVISION**

This field is used to enter the Pager ID number for Trouble reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***69 PAGER PHONE NUMBER FOR BYPASSES**

This field is used to enter the alpha numeric paging service phone number for Bypass reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***70 PAGER ID NUMBER FOR BYPASSES**

This field is used to enter the Pager ID number for Bypass reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***71 PAGER PHONE NUMBER FOR OPENS/CLOSES**

This field is used to enter the alpha numeric paging service phone number for Open/Close reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***72 PAGER ID NUMBER FOR OPENS/CLOSES**

This field is used to enter the Pager ID number for Open/Close reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***73 PAGER PHONE NUMBER FOR SYSTEM**

This field is used to enter the alpha numeric paging service phone number for System reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***74 PAGER ID NUMBER FOR SYSTEM**

This field is used to enter the Pager ID number for System reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***75 PAGER PHONE NUMBER FOR TEST**

This field is used to enter the alpha numeric paging service phone number for Test reports. Enter up to 17 digits, **0-9; enter #11 for *, #12 for #, and #13 for a 2-sec. pause.** Do not fill unused spaces. Enter ***** after the last digit of the phone number.

***76 PAGER ID NUMBER FOR TEST** | | | | | | | | | | |

This field is used to enter the Pager ID number for Test reports. Enter up to 10 digits. If fewer than 10 digits are required, enter ***** after the last digit, (i.e., pager pin number).

***79 ZONE TYPE RESTORES FOR ZONE TYPES 1-8** | | | | | | | | |

1 2 3 4 5 6 7 8

Enter **1** to enable Restore reporting for individual zone types.

Enter **0** if no Restore report is desired for a zone type. Default = 0.

***80 ZONE TYPE RESTORES FOR TYPES 9/10** | | |

9 10

Enter **1** to enable Restore reporting for individual zone types.

Enter **0** if no Restore report is desired for a zone type. Default = 0.

***83 FIRST TEST REPORT TIME [00, 12, 00]** | | | | | |

Enter the day (**00-07**) and time (**00-23 hours/00-59 min.**) 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.

**Note:** that day 01=Monday. See *Report Code Programming* (System Group 1) in the *#93 Menu Mode Programming* section for assigning the Test Report Code.

***84 SWINGER SUPPRESSION (partition-specific)** [03] | |

This option limits the number of messages (alarms or troubles) sent for a specific channel in an armed period (Swinger Suppression). Enter **01-15**. If **00** is selected, all alarm or trouble codes are reported.

Must be **00** (disabled) for UL installations.

***85 ENABLE DIALER REPORTS FOR PANICS & DURESS** [0] | | | | |

**(partition-specific)** 95 96 99 Duress

Enter **1** for each panic/duress for which reporting is desired.

**Note:** Non-zero report code must be assigned to zone 992 (duress) to enable Duress reporting.

***87 ENTRY WARNING (partition-specific)** [1] |

Enter **0** for 3 short beeps, or **1** for slow beeps that continue for the entire entry delay period.

***88 BURG. ALARM COMM. DELAY (partition-specific)** [0] |

Enter **0** for no delay on burglary alarm communication. Enter **1** for 16-second delay (no delay on 24-hour reports). Must be **0** for UL installations.

***89 RESTORE REPORT TIMING** [0] |

Enter **0** for instant Restore report as zone restores.

Enter **1** for reporting after bell timeout if zone restored. Enter **2** for Restore report when system is subsequently disarmed. Must be **2** for UL commercial burglary installation.

***90 SECONDARY SUBSCRIBER ACCT #** | | | |

**(partition-specific)** Enter 00-09; B-F (11-15) [15 15 15 15]

Enter the 3-or 4-digit number (depending on report format) for the secondary subscriber account: 00-09; B-F (11-15). Each number requires a 2-digit entry to allow entry of hexadecimal digits (B-F). If a 3-digit number is to be used, enter data only in the first 6 locations, leaving the last two unfilled. Default=15 15 15 15. Erase the field by entering *90*. 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]

Enter 1 to display the letters TRBL instead of CHECK when a zone or system trouble occurs.

Enter **0** to display CHECK.

**1*10 FIRE DISPLAY LOCK** [0]

**0** = scroll all alarms

**1** = lock display of first fire alarm (press ***** to display other alarms)

**1*17 LOBBY PARTITION** [0]

Enter the Common Lobby Partition **(1-8).**

Enter **0** if none.

**1*18 AFFECTS LOBBY (partition-specific)** [0]

Enter **1** if this partition affects the common lobby. Will cause lobby to disarm when this partition disarms.

Enter **0** if it does not.

**1*19 ARMS LOBBY (partition-specific)** [0]

Enter **1** if arming this partition causes the system to attempt to arm the common lobby partition automatically. Can only arm lobby if all other affecting partitions are armed. To enable this field, field 1*18 must also be enabled (partition-specific).

Enter **0** if arming this partition will not attempt to arm the common lobby partition.

**1*20 EXIT ERROR LOGIC ENABLE** [0]

Enter **1** to enable Exit Error Logic (entry/exit doors and interior zones will be bypassed if left open).

Enter **0** if Exit Error Logic is not desired. Must be **0** for UL commercial burglary installations.

**1*21 EXIT DELAY RESET** [0]

Enter **1** to reset exit delay to 60 seconds after door is closed.

Enter **0** if exit delay not to be reset. Must be **0** for UL commercial burglary installations.

**1*22 CROSS ZONING PAIR ONE** | |

Enter the first pair of zones, which must both be faulted within a five-minute period to cause an alarm.

Enter **00,00** to disable. Must be 00,00 for UL burglary installations.

**1*23 CROSS ZONING PAIR TWO** | |

Enter the second pair of zones, which must both be faulted within a five-minute period to cause an alarm.

Enter 00,00 to disable. Must be 00,00 for UL burglary installations.

**1*24 CROSS ZONING PAIR THREE** | |

Enter the third pair of zones, which must both be faulted within a five-minute period to cause an alarm.

Enter 00,00 to disable. Must be 00,00 for UL burglary installations.

**1*25 CROSS ZONING PAIR FOUR** | |

Enter the fourth pair of zones, which must both be faulted within a five-minute period to cause an alarm.

Enter 00,00 to disable. Must be 00,00 for UL burglary installations.

**1*26 PANIC BUTTON OR SPEEDKEY** [00,00,00,00] | | | | | | | |

**A B C D**

For each lettered key A-C, enter 00 to assign that key's respective panic function, or enter a speedkey macro number **01-32** to assign a particular macro to that key. For the **D** key, enter 00 to use the **D** key to select a macro to execute when key is pressed, or enter a macro number **01-32** to execute a particular macro with the **D** key.

Instead of the 32 macros, each key can be programmed for any of 3 other functions. **Choice 33** = fire sounder silence. The key, when pressed, will silence fire alarms.

**Choice 34** = display next fire alarm. The key, when pressed, will display the next fire alarm present in the system.

**Choice 35** = display previous fire alarm. The key, when pressed, will display the previous fire alarm present in the system.

**Note:** Choices 34 and 35 should be used in conjunction with field 1*10 Fire Display Lock.

**1*28 RF TX LOW BATTERY SOUND** [0] |

Enter **0** if display and audible beep annunciation upon RF transmitter low battery condition is desired only in disarmed state.

Enter **1** if audible beep and display is desired in both armed and disarmed states.

Must be **1** for UL.

**1*29 RF TX LOW BATTERY REPORTING** [0] |

Enter **1** if a Trouble message for RF transmitter low battery condition is to be sent to the central station.

Enter **0** if no report for transmitter low battery is desired. Note that a Trouble message will be sent for a transmitter supervision failure, independent of this selection.

Must be **1** for UL.

**1*30 RF RCVR SUPERVISION CHECK-IN INTERVAL** [06] [ | ]

Enter the check-in monitoring interval in 2-hour increments.

Enter **02-15** times 2 hours (4-30 hours). Failure of a receiver to receive any RF signal within the time entered will result in 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.

Enter **00** to disable receiver supervision.

Max. "2" (4 hr) for UL.

**1*31 RF TRANSMITTER CHECK-IN INTERVAL** [12] [ | ]

Enter the check-in monitoring interval in 2-hour increments.

Enter **02-15** times 2 hours (4-30 hours).

Failure of an individual transmitter to send a supervision signal within the time entered will result in a trouble response and related communication report. Enter **00** to disable transmitter supervision.

Max. "2" (4 hr) for UL.

**1*33 TOUCH-TONE W/ROTARY BACKUP** [0] [ ]

Enter **1** to enable rotary backup dialing if communicator is not successful in dialing using TouchTone DTMF on first attempt.

Enter **0** if this option is not desired.

**1*34 COMM. SPLIT REPORT SELECTION** [0] [ ]

This field allows certain reports to be directed to either the primary or secondary phone number.

Enter **0, 1, or 2,** in accordance with the following:

**0** = split reporting disabled;

**1** = Alarm, Alarm Restore and Cancel reports sent to primary telco number, all others to secondary telco number;

**2** = Open/Close and Test reports sent to secondary telco number and all other reports to primary;

See *51 for split/dual reporting combinations.

**1*35 ACCESS CONTROL DIALER ENABLES** [000000] [ ] [ ] [ ] [ ] [ ] [ ]

Trace Trbl Byp Not Used Systm Alm

Enter **1** for Trace to have the access grant/denial events sent to the central station.

Enter **1** to enable or **0** to disable each type of event.

**1*42 CALL WAITING DEFEAT** [0] [ ]

Enter **1** for the panel to defeat Call Waiting on the first attempt (DO NOT enable unless Call Waiting is being used).

Otherwise, enter **0**.

**1*43 PERMANENT KEYPAD DISPLAY BACKLIGHTING (partition-specific)** [0] [ ]

Enter **1** if backlighting for the keypad display is to remain on at all times.

Enter **0** if the display should remain unlit unless a key is pressed. The backlighting then turns off again after a period of keypad inactivity. Note that when a key is pressed, display backlighting turns on for **all** keypads in that partition.

**1*44 WIRELESS KEYPAD TAMPER DETECT** [0]

Enter **1** to enable tamper detection on wireless keypad.

Enter **0** if tamper detection is not desired. If this feature is enabled, any attempt to tamper by means of many trial entries at a wireless keypad will be blocked by the control panel. If more than 40 key depressions are received without a valid sequence (arm, disarm, etc.), the Control panel will disable the wireless keypad. The inhibit is removed once a valid key sequence is received from a wired keypad.

**1*45 EXIT DELAY SOUNDING (partition-specific)** [0]

Enter **1** if beeping from the keypads during exit delay are desired. Enter **0** for no keypad sound during exit delay.

**1*46 AUXILIARY OUTPUT MODE** [0]

Enter **0** if ground start output is required.

Enter **1** if the auxiliary output will be used to produce an open/close trigger (produced only if ALL partitions are armed).

Enter **2** if the auxiliary output will be used to produce keypad-like sounding at an auxiliary sounder (ex. 706-12). This option applies only to the partition enabled in field *15.

Enter **3** if AAV module is being used.

**NOTE:** Only one of the above options may be active within the system.

**1*47 CHIME ON EXTERNAL SIREN (partition-specific)** [0]

Enter **1** for chime annunciation using the external alarm sounder. If not desired, enter **0**.

**1*48 WIRELESS KEYPAD ASSIGNMENT** [0]

Enter the partition in which RF keypad is used, **1-8.**

Enter **0** if no RF keypad is used.

**1*49 SUPPRESS TX SUPERVISION SOUND** [1]

Enter **1** to disable trouble sounding for transmitter check-in failure.

Enter **0** if audible trouble sounding is desired.

Must be **0** for UL.

**1*52 SEND CANCEL IF ALARM + OFF (partition-specific)** [0]

Enter **1** if Cancel reports are to be sent when the system is disarmed after an alarm, regardless of how much time has gone by.

Enter **0** if Cancel reports are to be sent within Bell Timeout period only.

**1*53 DISABLE DOWNLOAD CALLBACK** [0]

Enter **1** to disable the callback requirement for downloading.

Enter **0** to require a callback.

Must be **0** for UL commercial burglary installations.

**1*56 AC 60Hz or 50Hz** [0]

Enter 1 for 50 Hz Standard or 0 for 60 Hz Standard. Must be set to **0** for U.S. installations (this is the default).

**1*57 ENABLE 5800 RF BUTTON GLOBAL ARM** [0] ☐

Enter **1** to have the system arm/disarm in accordance with the button's user's global arming settings.

Enter **0** if the button is not to be used to global arm the system (however, home partition arming will still occur).

**1*58 ENABLE 5800 RF BUTTON FORCE ARM** [0] ☐

Enter **1** to allow the RF button user to force a bypass of all faulted zones when arming the system. When attempting to arm the system, the keypad will beep once after pressing the button if any faulted zones are present. If this feature is enabled, the user should then press the button again within 4 seconds to force-bypass those zones and arm the system.

Enter **0** if RF button force bypass is not desired.

**1*60 ZONE 5 AUDIO ALARM VERIFICATION** [0] ☐

Enter **1** if 2-way audio (AAV) is being used.

Enter **0** if AAV is not being used. Must be 0 for UL installations.

**1*70 EVENT LOG TYPES**

| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
|---|---|---|---|---|---|
| Alm | Chck | Byps | O/C | Systm | Test |

Enter **1** for each type of event for which event logging is desired.

Otherwise enter **0**.

**Note:** Events will also be logged into the PassPoint system, if installed.

**1*71 12/24 HOUR TIME STAMP FORMAT** [0] ☐

Select the type of time stamping desired:

**0**=standard 12-hour; **1**= 24-hour format.

**1*72 EVENT LOG PRINTER ON-LINE MODE** [0] ☐

Enter **1** to have the printer print events as they occur.

Enter **0** to enable the printer such that the logs are printed only upon request.

**1*73 PRINTER BAUD RATE** [0] ☐

Enter **0** if printer is set for 1200 baud (preferred).

Enter **1** if printer is set for 300 baud.

Note: Must be **1** if using the alpha numeric pager interface.

**1*74 RELAY TIMEOUT XXX MINUTES** [000] | |

Enter the relay timeout, **000-127** in multiples of 2 minutes, desired for #80 Menu Mode time-driven event relay command numbers "04/09" and *Output Programming* in the *#93 Menu Mode Programming* output command "56" (refer to *#93 Menu Mode* and *Scheduling* sections in this manual).

**1*75 RELAY TIMEOUT YYY SECONDS** [000] | |

Enter the relay timeout, **000-127** seconds, desired for #80 Menu Mode time-driven event relay command numbers "05/10" *Output Programming* in the *#93 Menu Mode Programming* command "57" (refer to *#93 Menu Mode* and *Scheduling* sections in this manual).

**1*76 ACCESS RELAY # # (partition-specific)** [00] |

The system can be programmed to provide user-activated access control. If enabled, the assigned relay will pulse for 2 seconds when the user enters his code and presses 0. Enter the relay number (**00-96**) for the relay that will be used for access control. Enter **00** if not used in this partition. This function has not been UL Listed for use with the VISTA-128B control. Must be **00** for UL installations.

*****Note: See the *Access Control* section for enhanced access control capability.

**2*00 NUMBER OF PARTITIONS** [1]

Enter the number of partitions (**1-8)** to be used in the system.

**2*01 DAYLIGHT SAVING TIME START/END MONTH** [04,10] | |

Enter the months (**00-12)** in which daylight savings time starts and ends.

Enter **00, 00** if daylight savings time does not apply to the user's region. Standard setting for U.S. is 04,10.

**2*02 DAYLIGHT SAVING TIME START/END WEEKEND** [1,5]

Enter the start and end weekends for daylight savings 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 1,5.

---

**UL** Fields 2*05 – 2*08 must be set to 0 for UL installations.

---

**2*05 AUTO-ARM DELAY (partition-specific)** [15] |

Enter the time between the end of the arming window and the start of auto arm warning time in values of **01-14** times 4 minutes.

Enter **00** if no delay is desired.

Enter **15** if auto arming is not desired.

**2*06 AUTO-ARM WARNING PERIOD (partition-specific)** [15] |

Enter the time **01-15** in one-minute increments during which the user is warned by a keypad sounding and display to exit the premises prior to auto arming of the system.

Enter **00** to disable the warning period.

**2*07 AUTO-DISARM DELAY (partition-specific)** [15] |

Enter the time between the end of the disarming window and the start of auto disarming of the system in values of **01-14** times 4 minutes.

Enter **00** if no delay is desired.

Enter **15** if auto disarming is not desired.

**2*08 FORCE ARM ENABLE (FOR AUTO-ARM) (partition-specific)** [0]

Enter **1** if the system should automatically bypass any faulted zones when it attempts to auto arm. Otherwise enter **0**.

**2*09 OPEN/CLOSE REPORTS BY EXCEPTION (partition-specific)** [0] ☐

Enter **1** if Open/Close reports are to be sent **only if** the openings/closings occur **outside** the arm and disarm windows. Open reports will also be suppressed during the closing window in order to prevent false alarms if the user arms the system, then reenters the premises to retrieve a forgotten item. Note that openings and closings are still recorded in the event log. Enter **0** if exception reporting is not desired. Note: This field **must** be set to **1** if No Opening and No Closing reports are to be sent.

**2*10 ALLOW DISARMING ONLY DURING ARM/DISARM WINDOWS (partition-specific)** [0] ☐

Enter **1** if disarming of the system should be allowed only during the arming/disarming windows, or if the system is in alarm (if 2*11 is set to 1). Note that this applies **only** to operator level users. Installer, Master and Manager level users can disarm the system at any time. Enter **0** if disarming can occur at any time.

**0**=disable for displayed partition; **1**=enable for displayed partition

**2*11 ALLOW DISARM OUTSIDE WINDOW IF ALARM OCCURS** [0] ☐

Used only if field 2*10 (partition-specific field) is set to 1.

Enter **1** to allow the system to be disarmed outside the programmed disarm (opening) window if an alarm has occurred.

Enter **0** to allow disarming only during the disarm window, regardless of system status. If field 2*10 is set to 0 for a partition, this field (2*11) has no effect for that partition.

**2*18 ENABLE GOTO FOR THIS PARTITION (partition-specific)** [0] ☐

Enter **1** if this partition is to be accessed from another partition's keypad using the GOTO command. Otherwise enter **0**.

**2*19 USE PARTITION DESCRIPTOR** [0] ☐

Enter **1** if partition descriptors will be programmed. If enabled, the normal keypad display will include a partition number and four-digit descriptor).

Enter **0** to cause the keypads to display a nonpartitioned system type of display (no partition number will appear).

**2*20 ENABLE J7 TRIGGERS FOR PARTITION (partition-specific)** [1] ☐

**2*21 SUPERVISION PULSES FOR LRR** [000] ☐☐☐

F B S

Used for supervised connection to 7920SE.

Enter **1** to enable pulses for each type of LRR trigger (Fire, Burglary/Audible Panic, Silent Panic/Duress. This option causes the control to send periodic short pulses on the J7 radio triggers. These pulses are used by the 7920SE to determine that its connection to the control is still intact.

Enter **0** if not desired.

Must be **1** for UL commercial burglary installations.

**2*22 DISPLAY FIRE ALARMS OF OTHER PARTITIONS (partition-specific)** [0] ☐

Enter **1** to allow fire alarms that occur on other partitions to be displayed at this partition's keypad(s). Otherwise, enter **0**.

**2*23 DISPLAY BURG & PANIC ALARMS OF OTHER PARTITIONS** [0] ☐

Enter **1** to allow burglary and panic alarms that occur on other partitions to be displayed at this partition's keypad(s). Otherwise, enter **0.**

**2*24 DISPLAY TROUBLES OF OTHER PARTITIONS** [0] ☐

Enter **1** to allow troubles that occur on other partitions to be displayed at this partition's keypad(s). Otherwise, enter **0**.

# #93 Menu Mode Programming

## In This Section



## General Information

The #93 Menu Mode is a mode through which much of the system's programming is done. It enables the programming of the system via interactive screen prompts.

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.

**NOTE: The following field should be preset before beginning: 2*00 Number of Partitions. In addition, receivers should be programmed via Device programming.**

Below is a list of the main menu selections. For the detailed selections refer to the *VISTA-128B Programming Guide.*

Menu selections are as follows:

ZONE PROG?
1 = YES 0 = NO

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.

EXPERT MODE?
1 = YES 0 = NO

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

For programming the following:

- Alarm report codes for zones
- Restore & supervisory codes
- All other system report codes

ALPHA PROG?
1 = YES 0 = NO

For entering alpha descriptors for the following:

- Zone Descriptors
- Installer's Message
- Custom Words
- Partition Descriptors
- Relay Descriptors

| | |
|---|---|
| DEVICE PROG?<br>1 = YES 0 = NO | For defining the following device characteristics for addressable devices, including keypads, RF receivers (5881), output relay modules (4204/4204CF), 4285/4286 VIP Module, ECP long range radio (7820), and vista gateway module:<br>• Device Address<br>• Device Type<br>• Keypad Options (incl. partition assignment)<br>• RF House ID<br>• LRR Options (incl. programming radio) |
| OUTPUT PGM?<br>1 = YES 0 = NO | For defining output relay functions. |
| RLY VOICE DESCR?<br>1 = YES 0 = NO | For entering voice descriptors for relays to be used with the 4285/4286 VIP Module. |
| CUSTOM INDEX ?<br>1 = YES 0 = NO | For creating custom word substitutes for VIP Module annunciation. |
| ACCESS POINT PGM<br>1 = YES 0 = NO | 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 the detailed programming instructions. |
| ACCESS GRP PGM<br>1 = YES 0 = NO | For defining the capabilities (privileges) for each group of users. See the *VistaKey-SK Installation and Setup Guide* for the detailed programming instructions. |
| EVENT/ACTION PGM<br>1 = YES 0 = NO | For defining events and time windows for an access group. See the *VistaKey-SK Installation and Setup Guide* for the detailed programming instructions. |

# Scheduling Options

### In This Section



## Introduction to Scheduling

This section describes the scheduling features provided with this control panel.

---

**UL**

- You must program Bypass and Auto-Arm Fail reports for UL installations.
- Auto-disarming is not for use in UL installations.

---

### General

- The scheduling features allow certain operations to be automated, such as auto-arming, auto-disarming, auto-bypassing and unbypassing of zones, and activating relay outputs (using 4204 modules).
- 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 and #83 modes), explained in detail in this section. These menus take you step by step through the options.

### Auto Arming

- 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 begin to 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 will begin at the end of the extension.

### Force Arm

- The force arm option causes the panel to attempt to bypass any faulted zones prior to auto-arming (panel will perform 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, it is highly recommended to set 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.
- This option is set in partition-specific field 2*09.
- The system can be programmed to send No Opening and No Closing reports if the partition is not armed or disarmed by the end of the corresponding time window.

### Time-Driven Events

- By using the time windows, 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 the time window:
  1. At the beginning of a time window
  2. At the end of a time window
  3. During a time window active period only (on at beginning of window, off at end)
  4. 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)
- The system can perform the same actions on a daily basis, or can be made to perform an action only once (i.e., 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 on preset days.

### Limitation of Access of Users by Time

- A user's access can be limited to a certain time period, during which he can perform system functions. Outside this time, that user's code will be inactive.
- The system provides up to 8 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 for a given user when that user's access code is added to the system.
- If a user tries to operate the system outside of the schedule, the alpha keypad will display "Access Denied."

## Time Window Definitions

### General

- Scheduled events are based on time windows, which are simply periods of time during which an event may take place.
- A time window is defined by a “Start” time and a “Stop” time.
- The system supports up to 20 time windows.
- The windows are shared by all 8 partitions, and are used when programming the various schedules (open/close, limitation of access), as well as for time-driven event control.

### Scheduling Example

To understand scheduling, take, for example, a store that has the following hours:

| | |
|---|---|
| Monday to Thursday: | 9am to 6pm |
| Friday | 9am to 9pm |
| Saturday | 10am to 4pm |
| Sunday | Closed |
| Holidays | Closed |

Assume the owner desires the times to allow employees to arm or disarm the system:

| | | |
|---|---|---|
| Monday to Thursday: | Open (disarm)<br>Close (arm) | 8am to 9am<br>6pm to 6:30pm |
| Friday | Open (disarm)<br>Close (arm) | 8am to 9am<br>9pm to 9:30pm |
| Saturday | Open (disarm)<br>Close (arm) | 9am to 10am<br>4pm to 4:30pm |
| Sunday & Holidays | Closed | |

To provide these schedules, the following five 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-Thurs. close window |
| 5 | 9pm | 9:30pm | Friday close window |

Using the *#80 Menu Mode* (described later in this section), the installer can program open/close schedules by assigning each 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 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 will override 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 the *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 (a person who arms the system forgets something and has to reenter), 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.

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

### Example of Open/Close Exception Reporting & Scheduling

| **6:01PM 5:59AM** | **6AM 9AM** | **9:01AM 3:59PM** | **4PM 6PM** | **6:01PM 5:59AM** |
|---|---|---|---|---|
| Early Opening reports will be sent if system is manually disarmed before opening window begins.<br>** Early and Late Opening and Closing reports are programmable options in the Report Code programming section. They are not dependent on the programming of the Exception Reporting option.* | Opening Window<br>No reports sent if system disarmed during this time window.<br>*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.<br>Auto-disarm occurs after delay (if auto-disarm is enabled).<br>Missed Opening reports will be sent if manual disarming has not occurred at expiration of opening window.<br>Late Opening reports will be sent if disarm occurs after the opening window expires.<br>Early Closing reports will be sent if manual arming occurs before the closing window begins.<br>** Missed Opening/Closing type reports are programmed in the Report Code programming section. The Exception Reporting option must be set for these to be sent.* | Closing Window<br>No reports sent if system is armed* during this time window.<br>* or disarmed if user needs to re-enter premises. | Auto-arm delay begins.<br>Auto-arm warning begins.<br>Auto-arm occurs after warning expires (if auto-arm is enabled).<br>Missed Closing reports will be sent if manual arming has not occurred at expiration of closing window.<br>Late Closing reports will be 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. To enter this mode, the system must first be in the normal operating mode (all partitions disarmed). Enter **[User Code] + [#] + 8 + 0**. **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:

- Define time windows
- Assign open/close schedules to each partition
- Assign holiday schedules
- Program time-driven events (for system functions and relay activation)
- Assign limitation of access schedules

Some scheduling features are programmed in Data Field Programming Mode (**[Installer Code] + 8 0 0 0**). The general Programming Mode scheduling fields are listed below.

| | | |
|---|---|---|
| System-Wide Fields: | 1*74 -1*75 | Relay time-out values |
| | 2*01-2*02 | Daylight savings time options |
| | 2*11 | Allow disarming outside window if alarm occurs |
| Partition-Specific fields: | 1*76 | Access control relay for this partition |
| | 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 |
| Report Code Programming in #93 Menu Mode | | |
| (System Group #3) | | Scheduling related report codes |

Event-driven relay activation options are programmed using the *Output Programming* in the #93 *Menu Mode*. These actions are in **response** to a programmed action. However, relay activation can also be time-driven, and thus be used to initiate a desired action. Time-driven relay activation options are programmed using the *#80 Menu Mode*. Refer to the *Time-Driven Event Programming* for procedures.

### Steps To Programming 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:

- Define time windows (up to 20)
- Define the daily open/close schedules (one schedule per day, per partition)
- Define the holidays to be used by the system (up to 16)
- Define limitation of access times (up to 8 schedules)
- Define the time-driven events (up to 20)

**Note:** Temporary schedules are programmed using the #81 Menu Mode.

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

- Program the time windows
- Program the open/close schedules
- Program the time-driven events
- Program the access schedules

## Scheduling Menu Structure

To program schedules, enter Scheduling Program Mode:

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

This mode can only be entered when all partitions are disarmed.

There are 5 sections of scheduling menus, as shown below. Entering **1** at a displayed main menu prompt will select that menu section. Prompts for programming that scheduling feature will then appear. Enter **0** to skip a section and display the next menu option.

| | |
|---|---|
| Time Window ?<br>1 Yes 0 = No 0 | Upon entering Schedule Menu Mode, this prompt will appear. Enter **1** to program time windows. Refer to *Time Windows Programming* later in this section for detailed procedures.<br>Enter **0** to move to the "O/C Schedules?" prompt. |
| O/C Schedules ?<br>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.<br>Enter **0** to move to the "Holidays?" prompt. |
| Holidays ?<br>1 Yes 0 = No 0 | Enter **1** to program holiday schedules. Refer to *Holiday Schedule Programming* later in this section for detailed procedures.<br>Enter **0** to move to the "Timed Events?" prompt. |
| Timed Events ?<br>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.<br>Enter **0** to move to the "Access Sched?" prompt. |
| Access Sched. ?<br>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.<br>Enter **0** to move to the "Quit?" prompt. |
| Quit ?<br>1 Yes 0 = No 0 | Enter **1** to quit *#80 Scheduling Menu Mode* and return to normal operating mode.<br>Enter **0** to make any changes or review the scheduling programming options. If **0** is pressed, 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 8 partitions.

### Time Windows Worksheet

The following worksheet will help you define time windows and scheduling aspects of this system before programming the time window definitions for this installation. Note that time windows **can** span midnight.

| 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 will display the *Time Window Programming* prompt.

| |
|---|
| Time Window ?<br>1 Yes 0 = No 0 |

Enter **1** at this main menu prompt to program time windows.

| |
|---|
| Time Window # ?<br>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<br>00:00AM 00:00AM |

If a time window number was entered, the cursor will be positioned on the tens of hours digit of the start of window entry.

Enter the desired start of window hour and press [∗]. The cursor will move to the minutes. 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 ?<br>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.

Since 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

### Open/Close Schedule Worksheet

Write in the previously defined time window numbers for open & 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

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

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

```
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 will be 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 will be displayed.

Press the [*] key to accept the entry.

```
Tue  P1 OP WIND.?
00:00   00:00    00
```

The keypad will now prompt for Tuesday's open/close schedule, etc. 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 will override the regular daily open/close schedule on the programmed holidays throughout the year.

### Holiday Schedule Worksheet

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.

| 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.

```
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 will be 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 will be 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 are the schedules used to activate outputs, bypass zones, etc. based on a time schedule. There are 20 of these events that may be programmed for the system, with each event 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

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) **First 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 are 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 the *Output Programming* in the *#93 Menu Mode*.

#### Relay commands

| Action Code | 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

Activation times 1 (Beginning), 2 (End), 3 (During) are the only valid choices for automatic arming and disarming functions.

"During" can be used to arm and disarm the control for a specific time only. For example, if "during" is selected with Arm-STAY, the system automatically Arms-STAY at the beginning of the window and automatically disarms at the end of the window.

| Action Code | 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) |

- The auto-arm warning (field 2*06) applies when using time-driven events to auto-arm.
- Temporary schedules will 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

Activation times **1** (Beginning), **2** (End), **3** (During) are the only valid choices for bypass commands. If **3** (During) is selected for auto-bypassing, the system will bypass the zone(s) specified on a particular zone list at the beginning of the window and unbypass the zone(s) at the end of the window. If it is selected for auto unbypassing, the system will remove the bypass of the zone(s) at the beginning of the window and will restore the bypass of the zone(s) at the end of the window.

| Action Code | Action Specifier |
|---|---|
| 30 Auto bypass - Zone list | Zone list # |
| 31 Auto unbypass - Zone list | Zone list # |

### Open/Close Windows

Activation time **3** (During) is the only valid choice for these commands.

| Action Code | 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 |
| 50 Off-Normal Reminder<br>(Starts local keypad beeping if fire off-normal condition exists) | None |

### Access Control Commands (use only with VistaKey Modules)

| Action Code | 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 # |
| 73 Access Point Trigger On | Trigger # |
| 74 Access Point Trigger Off | Trigger # |

### Additional Commands

| Action Code | Action Specifier |
|---|---|
| 75 Run Macro | Macro # |
| 76 Run Script | Script # |
| 77 Access Point Group Enable | Group # |
| 78 Access Point Group Disable | Group # |

**3) Enter the desired activation time,** which refers to when the action is to take place relative to the time window. 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). This can be used in conjunction with the arm, disarm or bypass commands to control a part of the system during the window.<br>For example, if bypass is selected to activate during the window, the zones in the zone list will be 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 will pulse for 2 seconds at the beginning of the window, signaling the beginning of the coffee break. At the end of the window it will pulse again, signaling the end of coffee break. |

### Automatic Refresh Feature

The system automatically updates the status of all Time-Driven Events upon any of the following occurrences:

- Changing of the time or date via #63 mode
- Exiting #80 Scheduling Menu mode
- Exiting Program mode
- After a disconnect from the downloader
- On a power-up
- At Daylight Saving Time adjustment.

### Time-Driven Event Programming

The following schedules can be used to activate outputs, bypass zones, arm/disarm the system, etc. based on a time schedule. Up to 20 events can be programmed for the system. Time windows must first be defined in order to be used to trigger events.

**If using time-driven events to control relays, the following menu items must first be programmed using *Output Programming in the #93 Menu Mode*:**

| | |
|---|---|
| Enter Relay No. | (reference identification number) |
| Output Group | (if applicable) |
| Restriction | |
| Output Type | (4101SN, 4204, X-10, or FSA) |
| ECP Address | |
| Relay No. | if 4204 relays |

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

| 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 will then prompt 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 will display.

**Action Codes:**

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 actions **01-05** were selected, the prompt at the right will be displayed. Enter the relay number.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

**Action Specifier:**

| 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 actions **06-10** were selected, the prompt at the right will be displayed. Enter the relay group number.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

| 01 RELAY GRP # ? |
| --- |
| 00 |

**Action Codes:**

20=Arm-STAY
21=Arm AWAY
22=Disarm
23=Force Arm STAY
24=Force Arm AWAY
40=Enable Open Window by part.
41=Enable Close Window by part.

**Actions 21-24 and 40-41**

If actions **21-24** or **40-41** were selected, the prompt at the right will be displayed. 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 |

**Action Codes:**

30=Auto bypass - Zone list

31=Auto unbypass - Zone list

**Actions 30-31**

If actions **30-31** were selected, the prompt at the right will be displayed. Enter the zone list number that contains the zones to be bypassed or unbypassed.

**Action Specifier:**

```
01  ZONE LIST ?
ENTER 01-15        01
```

Press [∗] to accept entry. The "Time Window ?" prompt appears.

42=Enable Access Window for Access group(s)

**Action 42**

If action **42** was selected, the prompt at the right will be displayed. Enter the group number to which the time window will apply.

```
GROUP ? 12345678
HIT 0-8     X
```

Press [∗] to accept entry. The "Time Window ?" prompt appears.

50=Off-normal Reminder

**Action 50**

No action specifier is required for this action since the conditions that this will occur for are system-wide.

```
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 will be displayed.

Press [∗] to accept entry.

```
01 Active time ?
                0
```

Enter the activation time from **1-4** (listed below). As the number is keyed in, the activation time will be 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.

Press [∗] to accept entry.

```
Days ?  MTWTFSSH
Hit 0-8  x   x
```

The system will then ask for which days the event is to be activated.

Press **0** to toggle all days on or off; or else 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 required 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.

## 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 8 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 (1-8; i.e., 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, do the following:

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

| | |
|---|---|
| Access Sched. ?<br>1 Yes 0 = No 0 | Enter **1** to program access schedules. |
| ACCESS SCHED # ?<br>01-08, 00 = Quit 01 | Enter the access control schedule number between **01** and **08**.<br>Press [∗] to accept entry.<br>Enter **00** at the "Access Sched #?" prompt to quit the access control menus and display the Quit ? prompt. |
| MON A1 Window 1?<br>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 will be displayed.<br>Press [∗] to continue. |
| MON A1 Window 2 ?<br>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 will be displayed.<br>Press [∗] to continue. |
| TUE A1 Window 1?<br>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 ?<br>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 will be displayed. |

Press [∗] to continue.

| Hol A1 Window 2 ?<br>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 will be displayed.

Press [∗] to continue.

| Quit ?<br>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 will override 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.

### 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 | **Disarm Window** | | | | | | | |
| | Start Time HH:MM | | | | | | | |
| | Stop Time HH:MM | | | | | | | |
| | **Arm Window** | | | | | | | |
| | Start Time HH:MM | | | | | | | |
| | Stop Time HH:MM | | | | | | | |
| 3…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. Note that only users with authority level of manager or higher can program temporary schedules. A temporary schedule only affects the partition from which it is entered.

Temporary schedules can also be reused at later dates simply by scrolling (pressing [#]) to the "DAYS?" prompt (described below) and activating the appropriate days. This should be considered when defining daily time windows.

| |
|---|
| Mon DISARM WIND.<br>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 will be 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 will toggle 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 [#] will scroll you through the prompts without making any changes.

| |
|---|
| Mon ARM WINDOW<br>00:00AM 00:00AM |

This prompt is for entering the start and end times of the arm (closing) window for Monday.

The cursor will be positioned on the tens of hours digit of the start time of the arm 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 will toggle the AM/PM indication.

Repeat the procedure for the stop time entry.

After the windows for that day have been completed, the system will prompt for disarm and arm time windows for the next day.

Press [#] if no changes are desired.

| |
|---|
| Tue DISARM WIND.<br>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 will prompt which days of the schedule are to be activated.

| |
|---|
| Days ? MTWTFSS<br>Hit 0-7 x x |

This is the prompt that actually activates the temporary schedule.

To select the days which are to be activated, enter **1-7** (Monday = 1). An "X" will appear under that day, indicating the temporary schedule for that day is active. Entering a day's number again will deactivate that day. Pressing **0** will toggle all days on/off.

The temporary schedule will only be in effect for the days which have 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 will 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" which will be available to the end user for the purpose of controlling output devices (4204 relay). These timers are comparable to the individual appliance timers that might be purchased at a department store. 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 relays to be "restricted" during*Output Programming in the # 93 Menu Mode*. These relays may not be controlled by the end user (this prevents the end user from controlling doors, pumps, bell outputs, etc.)

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

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

| | |
|---|---|
| 06 ON TIME ?<br>07:00 PM | The cursor will be positioned on the tens of hours digit of the ON time. Enter the desired hour.<br>Press [∗] to move to the minutes field. The minutes are entered in the same manner.<br>The AM/PM indication is toggled by hitting any key in the **0-9** range while the cursor is under the AM/PM position.<br>Press [∗] to continue. |
| 06 OFF TIME ?<br>11:45 PM | The cursor will be positioned on the tens of hours digit of the OFF. Enter the desired hour.<br>Press [∗] to move to the minutes field. The minutes are entered in the same manner.<br>The AM/PM indication is toggled by hitting any key in the **0-9** range while the cursor is under the AM/PM position.<br>Press [∗] to continue. |

| 06 DAYS? MTWTFSS |
| --- |
| HIT 0-7 x x |

To select the days which are to be activated, enter **1-7** (Monday = 1). An "x" will appear under that day, indicating the output for that day is active. Entering a day's number again will deactivate that day. Pressing **0** will toggle all days on/off.

The outputs will only be in effect for the days which have 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. An answer of **0** means that this schedule will be in effect for one week only. The letter "x" under the day will then be cleared, but all other entries for the output device will remain programmed.

Press [∗] to accept entry.

The system will quit User Scheduling Mode and return to normal operating mode.

# System Communication

## In This Section



## General Information

The VISTA-128B provides one main built-in dialer for communication to the central station. The communicator will make up to 8 attempts to transmit a report to one or both telephone numbers, depending upon the report routing option programmed. The control panel will transmit reports in the following order: alarms (fire, medical/panic, and burglary), remaining types of messages.

## Telephone Line Connections

Connect the main dialer output to telephone company lines which provide loop start service using the RJ31X cables supplied. *Do not* connect to telephone company lines which provide ground start service.

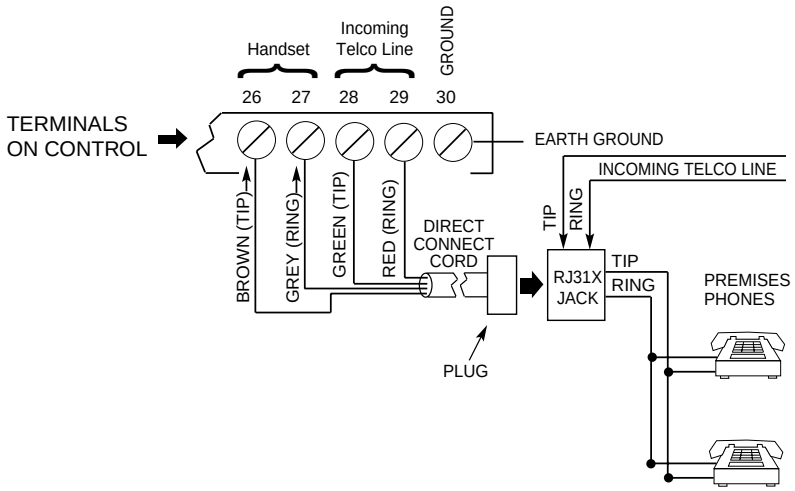



***Figure 25-1: Standard Telephone Line Connections***

- To prevent the risk of shock, disconnect phone lines at telco jack before servicing the panel.
- If the communicator is connected to a telephone line inside a PABX, be sure the PABX has a back-up power supply that can support the PABX for 24 hours (Central Station usage) or 60 hours (Remote Station usage). Many PABXs are *not* power backed up and connection to such a PABX will result in a communication failure if power is lost.

**UL**

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

### A Successful Transmission

When a control panel calls the central station receiver, it waits to hear a "handshake" frequency from the receiver to confirm that the receiver is on-line and ready to receive its message. Once the panel hears the handshake it is programmed to listen for, it sends its message. The panel then waits for a "kissoff" frequency from the receiver acknowledging that the message was received and understood.

Once the handshake frequency is received and understood by the panel, the panel will send its message. If there is an error in the transmission (the receiver does not receive a "valid" message), the central station receiver will not give the kissoff frequency.

The panel will make a number of attempts to the primary telephone number and a number of attempts to the secondary telephone number (if programmed) to get a valid message through. The number of attempts that are made to each number is set to 8 for each phone number. If the panel is not successful after its numerous attempts, the keypad will display "Comm Failure."

## Reporting Formats

The following chart defines the three sets of (handshake/kissoff) frequencies that the panel supports and the different formats that can be sent for each.

| FORMAT TIME | HANDSHAKE | TRANSMITS DATA | KISSOFF | TRANSMIT |
|---|---|---|---|---|
| Low Speed<br>3+1<br>4+1<br>4+2 | 1400Hz | 1900Hz (10PPS) | 1400Hz | Under 15 secs.<br>(Standard report) |
| Sescoa/Rad<br>3+1<br>4+1<br>4+2 | 2300Hz | 1800Hz (20PPS) | 2300Hz | Under 10 secs.<br>(Standard report) |
| Express<br>4+2 | 1400–2300Hz | DTMF (10 cps) | 1400Hz | Under 3 secs. |
| High Speed | 1400–2300Hz | DTMF (10 cps) | 1400Hz | Under 5 secs. |
| Contact ID | 1400–2300Hz | DTMF (10 cps) | 1400Hz | Under 3 secs. |

**ADVISORY:** ADEMCO's Contact ID reporting is capable of uniquely reporting all 128 zones of information, as well as openings and closings for all 128 users, to central stations equipped with the ADEMCO 685 receiver using software level 4.4 or higher. Must be level 4.7 or higher to fully support all new VISTA-128B report codes. 685 software levels below 4.4 cannot support Contact ID reporting. If you need to update your 685 receiver, contact your distributor.

**The following describes each format in greater detail.**

| | |
|---|---|
| **3+1 and 4+1 Standard Formats** | Comprised of a 3- (or 4-) digit subscriber number and a single digit report code (e.g. Alarm, Trouble, Restore, Open, Close, etc.). |
| **3+1 and 4+1 Expanded Formats** | Comprised of a 3- (or 4-) digit subscriber number, and a two-digit report code. The first digit is displayed on the first line, followed by a second line where the first digit is repeated 3 (or 4) times and followed by the second digit. This is the "expanded" digit. |
| **4+2 Format** | Comprised of a 4-digit subscriber number and 2-digit report code. |
| **ADEMCO Contact ID Reporting Format** | Comprised of a 4-digit subscriber number, 1-digit event qualifier ("new" or "restore"), 3-digit event code, 2-digit Partition Number, and 3-digit zone number, user number, or system status number. |
| **ADEMCO High Speed** | Comprised of 13 digits as follows: A 4-digit account number + eight channels of zone information (1-8 or duress plus 9-15) + one status channel, which identifies the type of events being reported in the eight zone locations. |

| Report | 3+1/4+1 Standard | 3+1/4+1 Expanded | 4+2 Low Spd or Express |
|---|---|---|---|
| Alarm | SSS(S) A | SSS(S) A<br>AAA(A) Z | SSSS AZ |
| Trouble | SSS(S) T | SSS(S) T<br>TTT(T) t | SSSS Tt |
| Bypass | SSS(S) B | SSS(S) B<br>BBB(B) b | SSSS Bb |
| AC Loss | SSS(S) E | SSS(S) E<br>EEE(E) $A_C$ | SSSS $EA_C$ |
| Low Batt | SSS(S) L | SSS(S) L<br>LLL(L) $L_B$ | SSSS $LL_B$ |
| Open | SSS(S) O | SSS(S) O<br>OOO(O) U | SSSS OU |
| Close | SSS(S) C | SSS(S) C<br>CCC(C) U | SSSS CU |
| Test | SSS(S) G | SSS(S) G<br>GGG(G)g | SSSS Gg |
| Restore Alarm | SSS(S) R | SSS(S) R<br>RRR(R) Z | SSSS RZ |
| AC Restore | SSS(S) $R_A$ | SSS(S) $R_A$<br>$R_AR_AR_A(R_A)A_c$ | SSSS$R_A$ $A_c$ |
| LoBat Res. | SSS(S) $R_L$ | SSS(S) $R_L$<br>$R_LR_LR_L(R_L)L_B$ | SSSS $R_LL_B$ |
| Trouble Res. | SSS(S) $R_T$ | SSS(S) $R_T$<br>$R_TR_TR_T$ $(R_T)$t | SSSS $R_T$t |
| Bypass Res. | SSS(S) $R_B$ | SSS(S) $R_B$<br>$R_BR_BR_B$ $(R_B)$b | SSSS $R_B$b |

***Where:***

SSS or SSSS = Subscriber ID
A = Alarm Code-1st digit
Z = Typically Zone Number*-2nd digit
Tt = Trouble Code 1st & 2nd digits
Bb = Bypass Code 1st & 2nd digits
$EA_C$ = AC Loss Code 1st & 2nd digits
$LL_B$ = Low Battery Code1st & 2nd digits
O = Open Code-1st Digit
C = Close Code-1st Digit
U = User Number (1st & 2nd digits)
Gg = Test Code (1st & 2nd digits)
R = Restore Code (Alarm) 1st & 2nd digits
$R_T$t = Restore Code (Trbl) 1st & 2nd digits
$R_B$b = Restore Code (Byps) 1st & 2nd digits
$R_AA_C$ = Restore Code (AC) 1st & 2nd digits
$R_LL_B$ = Restore Code (Bat) 1st & 2nd digits

*Zone numbers for: [✳] + [#], or [B] = 999; [3] + [#], or [C] = 996; [1] + [✳], or [A] = 995; Duress = 992

**ADEMCO High Speed Reporting** events by channel:

Channels 1 through 8 could have one of the following conditions:

1 = NEW EVENT
2 = OPENING (Status Channel Always = 2)*
3 = RESTORE
4 = CLOSING (Status Channel Always = 4)*
5 = NORMAL, NO EVENT TO REPORT
6 = PREVIOUSLY REPORTED, NOT YET RESTORED

* NOTE: Channel 1 will contain the user ID 1-9, A-F if Open/Close reporting is enabled.

The status channel might have one of the following conditions:

1 = DURESS (For Duress Plus Channels 9-15 Only)
2 = OPENING
3 = BYPASS (For Channels 1-8 Only)
4 = CLOSING
5 = SUPERVISORY/TROUBLE (For Channels 1-8 Only)
6 = SYSTEM STATUS:

- AC LOSS in Channel 1
- LOW BATTERY in Channel 2
- TIME SET in Channel 3
- LOG CLEAR in Channel 3
- LOG 50% FULL in Channel 3
- LOG 90% FULL in Channel 3
- LOG OVERFLOW in Channel 3
- POWER ON RESET in Channel 4
- WALK-TEST START, END in Channel 8

7 = NORMAL ALARM STATUS (Channels 1-8 Only)
9 = TEST REPORT

**Explanation of Channels 9-15:**

If there is a 1 in the status channel, and:

1 in the 1st location = Duress
1 in Channels 9-15 = Zone alarm on those channels
3 in Channels 9-15 = Restore on those channels
6 in Channels 9-15 = Previously reported alarm–not restored

A typical high speed report may look like this:

1234 5115 5555 7 (Acct #1234 with alarms on channels 2 and 3)
1234 5555 1555 1 (Acct #1234 with alarm on channel 12)

### LIMITATIONS

1. When using ADEMCO High Speed, remember there are only 15 channels available, plus a duress channel. If more than 15 zones are being used, they will have to share channels.
2. With ADEMCO High Speed reporting, channels 9-15 cannot report troubles or bypasses. Use these channels for zones that will not report these conditions.
3. Only user numbers 1-15 can be uniquely reported with Open/Close reports in ADEMCO High Speed.

**ADEMCO Contact ID Reporting** takes the following format:

CCCC QEEE GG ZZZ

CCCC = Customer (subscriber) ID

Q = Event qualifier, where:

E = new event, and R = restore

EEE = Event code (3 hexadecimal digits)

GG = Partition number (system messages show "00")

ZZZ = Zone number for an alarm, or user number for Open/Close reports. System status messages (AC Loss, Walk-Test, etc.) contain zeroes.

## TABLE OF CONTACT ID EVENT CODES

| Code | Definition |
|---|---|
| 110 | Fire 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 |
| 142 | Polling Loop Short Alarm |
| 150 | 24-Hour Auxiliary |
| 301 | AC Loss |
| 302 | Low System Battery |
| 305 | System Reset |
| 306 | Program Tamper |
| 308 | System Shutdown |
| 309 | Battery Test Fail |
| 310 | Ground Fault |
| 313 | System Engineer Reset |
| 320 | ACS Relay Supervision |
| 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 |
| 354 | ACS RS232 Fail |
| 373 | Fire Loop Trouble |
| 374 | Exit Error by Zone |
| 380 | Trouble (global) |
| 381 | Loss of Supervision (RF) |
| 382 | Loss of RPM Supervision |
| 383 | RPM Sensor Tamper |
| 384 | RF Transmitter Low Battery |
| 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 |

| Code | Definition |
|---|---|
| 409 | Keyswitch O/C |
| 411 | Callback Requested |
| 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 |
| 457 | Exit Error by User |
| 459 | Recent Close |
| 501 | ACS Reader Disable |
| 520 | ACS Relay Disable |
| 570 | Bypass |
| 576 | ACS Zone Shunt |
| 577 | ACS Point Bypass |
| 602 | Communicator Test |
| 606 | Listen-In to Follow |
| 607 | Burglary Walk-Test |
| 621 | Event Log Reset |
| 622 | Event Log 50% Full |
| 623 | Event Log 90% Full |
| 624 | Event Log Overflow |
| 625 | Time/Date Reset |
| 631 | Exception Schedule Change |
| 632 | Access Schedule Change |

# Downloading Primer

***(Remote Downloading is not a UL Listed feature)***

## In This Section



## General Information

Downloading allows the operator to remotely access, program, and control the security system over normal telephone lines. 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. An IBM PC compatible 486 33MHz PC or better with 30 MB of available hard disk space and at least 8MB of RAM (12MB is preferred). Windows 3.X, Windows 95, or Windows NT.
2. One of the following modems:
   - 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.*
3. COMPASS DOWNLOADING software may be purchased from ADEMCO. This software is available on 3-1/2" diskettes or CD ROM, and includes a complete User's Manual. It may also be downloaded from the ADEMCO web page. The web address is http://www.ademco.com.

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

Alternatively, you may use a 4100SM interface module to "direct-wire" the control panel to your computer at the site.

## Getting On-Line with a Control Panel

At the protected premises, the Control panel must be connected to the existing telephone line (refer to the *System Communication* section). No programming of the panel is required before downloading to an initial installation.

To download, do the following:

| 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 | Call the panel using the downloader software set to "First Communication" Mode.<br>The downloader will establish a session with no callback. The panel information can then be downloaded. |
| 3 | The downloader will establish a session with no callback. The panel information can then be downloaded.<br>a. The computer calls up the control panel. (The phone number for each customer is entered into the customer's account file on the computer.)<br>b. The control panel "answers" at the pre-programmed ring count and executes a handshake with the computer.<br>c. The computer sends a request for callback to the control, unless callback is not required.<br>d. The panel acknowledges the request and hangs up. During the next few seconds, the control will process the request, making sure certain encrypted information received from the computer matches its own memory.<br>e. Upon a successful match, the control panel will seize the phone line and call 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.)<br>f. The computer answers, usually by the second ring, and executes a handshake with the panel.<br>g. The panel then sends other default information to the computer. If this information matches the computer's information, a successful link is established. This is known as being “On-line.” |

- 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 will report immediately. All other reports will be 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.

## On-Line Control Functions

The following functions can be performed while on-line with a control panel:

- 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 (non-payment of monitoring fees in an owned system)

- Shut down all security system functions (non-payment for a leased system)
- Inhibit local keypad programming (prevents takeover of your accounts)
- Leave a message for customer
- 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, 512 event log, list of zones currently in alarm, list of zones currently in trouble, and ECP equipment list
- Set the real-time clock

## Access Security

Accessing the control from a remote location is protected against compromise by the use of 4 levels of protection:

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 Call-back: The control panel will "hang up" and call 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 downloading, the keypad displays "MODEM COMM."
- After each download or a save, an automatic time stamp is done, indicating the date and time of 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.

## Connecting a 4100SM Module for Direct Wire Downloading

The VISTA-128B can be downloaded without using a modem or telephone line, but by using a 4100SM Serial Module and Compass Downloading Software. The direct-wire downloading connection is to be temporary, and is not part of the permanent installation. Direct-wire downloading is meant as a tool for the installer during the installation process.

**The connections between the control and the 4100SM are different than those shown in the 4100SM Installation Instructions.** See the diagram below for correct connections. In addition, the green wire is referred to in step 2 of the "IN CASE OF DIFFICULTY" section of the 4100SM Instructions, **use the violet wire instead.**

Connector J8 on the main PC board (see the *Summary of Connections* diagram on the inside back cover of this manual), is intended to be interfaced to either a local serial printer (see *Event Log printer Connections* in the *Event Log Options* section) or a computer. Make connections to a computer as shown below. **Note that the violet wire connection for a computer differs from that used when connecting a serial printer.**

Remove the alpha numeric pager interface if it is installed while performing the direct-wire download. It may be reconnected once the direct-wire download is completed

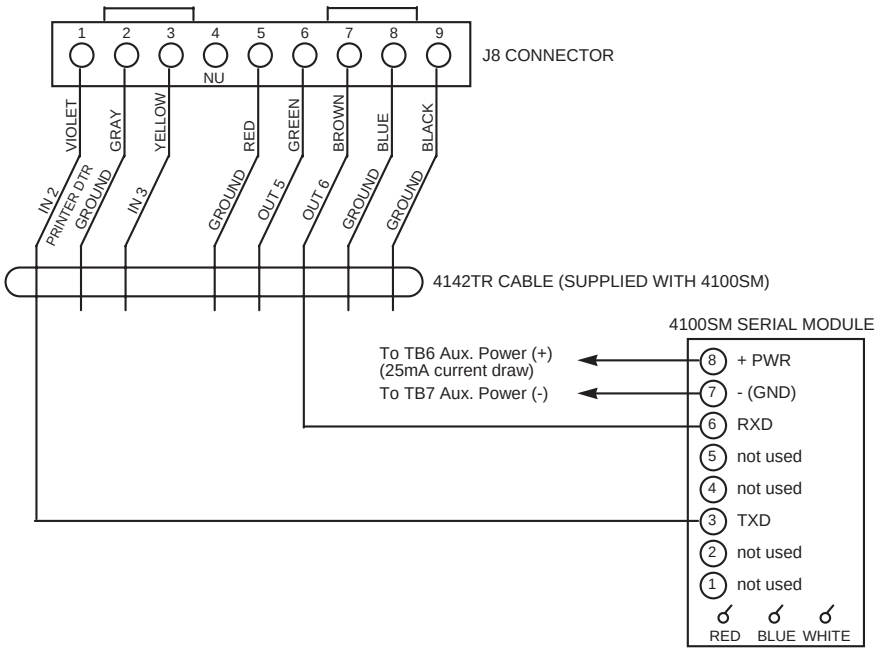



***Figure 26-1. Direct Wire Downloading Connections***

# Setting The Real-Time Clock

### In This Section



## 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 6139 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 real-time clock.

## Setting the Time and Date

To set the time and date, perform the following steps:

| Step | Action |
|---|---|
| 1 | Enter Installer or Master Code + **# 63**. Typical display shows:<br>TIME/DATE — THU<br>12:01 AM 01/01/90 |
| 2 | 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.<br>• Press [∗] to accept the entered value. The cursor then moves to the right.<br>• Press [#] to move the cursor to the left of the display, to the previous position.<br>• Enter the correct hour. Then press [∗] to move to the “minutes” field and make the correct entry.<br>• Press [∗] again, then press any key 0-9 to set AM/PM. Press any key again to change AM to PM, or PM to AM.<br>• Press [∗] to move cursor to the “month” field position and enter the correct month using a 2-digit entry.<br>• Press [∗] and enter the correct date.<br>• Press [∗] and enter the correct year. |
| 3 | Exit Clock Mode by pressing [∗] after the cursor is in the year position. |

# User Access Codes

### In This Section



## General Information

This system allows a total of 150 security access codes to be allocated, each 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 particular 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), which allows the [#] key to be pressed instead of entering the security code when arming the system. The security code must always be entered to disarm the system.

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

## User Codes & Levels of Authority

Each user of the system can be assigned a level of authority, which tells the system what system functions that user is authorized to do. A user can have different levels of authority within different partitions. In general, users can perform most system functions, including Test and Chime Modes, but certain authority levels restrict disarming, bypassing or the assigning of other user codes. These restrictions are noted in the descriptions below.

Use the "View Capabilities" keypad function to view the partitions and authority levels for which a particular user is authorized. These levels are described in the table below in order from highest to lowest ranking.

| Authority | Title |
|---|---|
| **0** | Installer |
| **1** | Master |
| **2** | Manager |
| **3** | Operator level A |
| **4** | Operator level B |
| **5** | Operator level C |
| **6** | Duress |

**Level 0: Installer (User 1) Code**

- Programmed in field *00 (default = 4-1-4-0). Installer Open/Close reporting is 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 codes of all other authority levels, 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. The only way to access Programming Mode if this done is by powering down the system, powering up again, and then pressing both the [*] and [#] keys at the same time within 30 seconds of power up.)
- 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 141 lower-level codes, which can be used by other users of the system.
- Cannot assign anybody a level of 0 or 1.
- May change his 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 of added users are is 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 his own code.
- Open/Close reporting of added users are is the **same** as that of the Manager who is adding the new user.

**Levels 3-5: Operator Codes**

- Can arm and disarm the system to the authority assigned, but cannot add or modify any user code.
- May operate a partition with one of the three Operator authority levels A through C in the 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 have the 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 (only useful if the system is connected to a central station).
- When the system's Auxiliary Voltage Triggers are connected to another communication's media (Derived Channel/Long Range Radio), 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.
- Will disarm (or arm) the system, but will also send a silent alarm to the central station (if service is connected). There will be no indication at the keypad that an alarm was sent.

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 will not be triggered if the 5th key is a [*], such as when performing a GOTO or viewing the capabilities of a user.

**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 & 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 only be DELETED or CHANGED 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.

**Open/Close Reporting Note:** When adding a user, the system will only prompt for Open/Close reporting capability if the user is being added by the Installer. When a Master or Manager adds a new user, the new user's Open/Close reporting enable will be 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 Examples

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 #3, the VP of Engineering, could be assigned to work within the Engineering Department (Partition 1) of ABC Manufacturing. Since he needs the full capabilities in his area, he is assigned as a MASTER with Level 1 authority. This means he may arm, disarm, bypass, add or modify users in Partition 1.

He must also be able to gain access to the manufacturing area (Partition 2) on an emergency basis. You can set this up easily with the partitioned system by requesting that he also be assigned to Partition 2, with a level of authority set lower, such as Level 4 (OPERATOR Level B), which allows him to arm and disarm, but nothing else. The control will automatically assign him the same user number within Partition 2, and does not require reprogramming of his already-existing 4-digit security code.

**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 will be ignored. However, panic key depression will cause an alarm and terminate user entry.

Enter **[Installer Code]†+ 8 + [new user # (002-150)] + [new user's code]**

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

Keypad will prompt for the authority level for this user.

| |
|---|
| User Number = 003 |
| Enter Auth. Level |

Enter the level number as follows:

1 = Master (arm, disarm, bypass, add or modify lower-level users)

2 = Manager (arm, disarm, bypass, add or modify lower level users)

3 = Operator Level A (arm, disarm, bypass)

4 = Operator Level B (arm, disarm)

5 = Operator Level C (arm, disarm only if system armed with this code)

6 = Duress (arm, disarm, trigger silent panic alarm)

Keypad will then prompt for Open/Close reporting option for this user.

| | |
|---|---|
| Open/Close Rep.?<br>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. |
| Access Group?<br>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 ?<br>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 will appear. Press **0** (NO) or **1** (YES). |
| Enter Button ZN #<br>(001-087) | If "yes" was given as the answer to the RF button question, the zone number for the button will be requested. Enter any one of the zone numbers assigned to the button transmitter as AWAY, STAY or DISARM. The system will then assign **all** buttons of the transmitter to this user number. |
| Multi-Access ?<br>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 ?<br>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 (described in the *Keypad Functions* section).<br>The keypad now prompts for the user's access to the next partition. |
| Part. 2 – SHOP ?<br>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.<br>If YES, the keypad prompts for the following:<br>• User's authority level in the displayed partition (see Authority Level prompt above).<br>• Open/Close option for this user in the displayed partition (see Open/Close prompt above).<br>• Global Arm option for this user in the displayed partition.<br>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. For example: |
| Part. 1 A0* WHSE<br>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 "✳" indicates the partition from which the user may be changed or deleted. |

## Changing a Master, Manager, or Operator Code

Enter **[Installer code]* + 8 + [User number (002-150)] + [new user's code]**

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

| |
|---|
| User Number = 003 |
| NEW USER? |

The system detects that the user number is already assigned, and will prompt if this is a new user.

Press **0** (NO).

The system will then confirm 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 "To ADD a Master, Manager, or Operator Code" paragraph.

## Deleting a Master, Manager, or Operator Code

Enter **[your code]* + 8 + [User number (002-150)] + [your code again]**

* Installer, Master or Manager Code, but must be code with higher level of authority than the code being deleted (i.e. Master Code can delete a Manager or Operator-level Code, but cannot delete another Master Code; a Manager Code can delete an Operator-level Code, but cannot delete a Master or another Manager Code).

| |
|---|
| OK TO DELETE 003? |
| 0=NO 1=YES |

The system will prompt to confirm that you want to delete this user. Press **0** (NO) or **1** (YES).

If “yes”, that user's code will be removed from all partitions to which it was assigned, and all authorization levels and other information about that user will be deleted. Note that a user can only be deleted by a user with a higher authority level. A user cannot delete himself.

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

## To EXIT the User Edit Mode

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

# Keypad Functions

### In This Section



## General Information

The keypad allows the user to arm and disarm the system, and perform other system functions, such as bypassing zones, viewing messages from the central station, and displaying zone descriptors. The system conditions are shown in the display window.

When an alarm occurs, keypad sounding and external sounding will occur, and the zone(s) in alarm will be displayed on the keypad. Disarming the system (enter the security code and press the OFF key) will silence both keypad and external sounders. After the system is disarmed, the system displays any zones that were in an alarm condition during the armed period. To clear this display, simply repeat the disarm sequence.

The keypads also feature chime annunciation, and 3 panic keys (for silent, audible, fire or personal emergency alarms) which can notify the central station of an alarm condition, if that service is connected.

## Arming Commands

The following is a brief list of arming commands. For detailed information concerning these functions, refer to the User's Manual.

| | |
|---|---|
| **Display Faulted Zones** | To arm the system must be in the READY condition (all zones must be intact). If the "NOT READY" message appears, press the READY * key to display faulted zones. |
| **Arming Away** | Enter code + 2 (AWAY) |
| **Arming Stay** | Enter code + 3 (STAY) (all zones designated as zone types 4 and 10 will be automatically bypassed). |
| **Arming Instant** | Enter code + 7 (INSTANT) (same as STAY without entry delay). |
| **Arming Maximum** | Enter code + 4 (MAXIMUM) (same as AWAY without entry delay). |
| **Disarming** | Enter code + 1 (OFF). |
| **Quick Arming** | Note that if QUICK ARM is enabled (field *29), the # key can be pressed instead of entering the security code, for any of the arming procedures (Away, Stay, Instant, Maximum, etc.). |

A user code other than the Installer Code must be programmed into the system in order for the Quick Arm feature to work.

**SUMMARY OF ARMING MODES**

| Mode | Features for Each Arming Mode | | | |
|---|---|---|---|---|
| | Exit Delay | Entry Delay | Perimeter Armed | Interior Armed |
| AWAY | Yes | Yes | Yes | Yes |
| STAY | Yes | Yes | Yes | No |
| INSTANT | Yes | No | Yes | No |
| MAXIMUM | Yes | No | Yes | Yes |

### Global Arming

If enabled for the user, the keypad will display the following:

```
ARM ALL     ?
0 = NO , 1 = YES
```

If NO, the keypad prompts for arming each partition individually. If YES, the system attempts to arm all partitions allowed by this user. If there are any faults (open doors, windows, etc.) the keypad will display them. See notes below. These faults must be corrected or the zone bypassed before arming will occur. When faults are corrected, repeat the arming procedure.

**Notes:**

- When using the Global Arm feature, if there are faults in any of the selected partitions, the system will enter a Summary Mode in which the faulted zones of all of the selected partitions will be displayed. These faults must be corrected or bypassed (code + BYPASS + [#] will attempt to bypass the faults in all of the selected partitions). This Summary Mode will end in approximately 120 seconds if no keys are pressed.
- If you are disarming the system using a Global Disarm, any of the selected partitions has a condition which would cause the keypad to beep (such as alarm memory or a trouble condition) the system enters a Summary Mode whereby the alarm memory or trouble conditions of all of the selected partitions is displayed. This mode continues until either approximately 120 seconds elapses or a second disarm occurs which clears the beeping.

### Bypassing and Chime Mode Commands

| | |
|---|---|
| **Bypassing Zones** | Enter code + 6 (BYPASS) + 3-digit zone number. To automatically bypass all faulted zones, use "Quick Bypass" method: Enter code + BYPASS + #. |
| **Chime Mode** | Enter code + 9 (CHIME). To turn Chime Mode off, enter code + CHIME again. |

## Access Control

The system has the capability to utilize access control by one of 4 methods.

1. One relay may be used for access control in each partition. The relay is programmed in data field 1*76. To activate this relay, the user enters his User Code + [0]. The relay will pulse for 2 seconds.
2. For a more powerful method of access control, program input devices (keypads, RF buttons, hardwired) and access points (using VistaKey or PassPoint ACS) (see the *Access Control* section). Up to 32 access point devices (relays) among 8 partitions can be controlled. For example, if a keypad is programmed as an access input device, then entering **[User Code] + [#73]** or **[User Code] + [#74]** will activate the appropriate access point relays (see also *Zone Programming* and *Output Programming* in the *#93 Menu Mode* section of the *Programming Guide*).
3. If a Vista Gateway Module along with the ADEMCO PassPoint Access Control System or a VistaKey module is installed, then these same inputs will automatically control the appropriate access points. Entering **[User Code]** + **[#75]** will control the state (protect, bypass, grant) of a door. (see the *Access Control* section).
4. If a VistaKey module is installed, entering **[User Code] + [#77]** enables the user to instantly perform an access control function. See the *VistaKey-SK Installation and Setup Guide* for a detailed explanation of these functions.

## Delaying Closing Time

If open/close schedules are used, end users can manually delay closing time by extending the closing window by 1 or 2 hours. This is useful if a user must stay on the premises later than usual. The user must have an authority level of Manager or higher.

To extend the closing window, enter **[User code] + [#] +82**.

| Closing Delay ? |
| --- |
| Hit 0-2 Hours |

Enter the number hours, **1** or **2**, by which the end of the closing window should be extended. Note that the delay is from the scheduled closing time, not from the current time.

Press [*] to accept entry and exit this mode. Press [**#**] to exit this mode without changes.

The system will send an Access Schedule Change report to the central station when the closing window is extended (if programmed).

An extension of the closing window cannot be reduced once it is set. However, a 1-hour delay can be increased to 2 hours. This is to prevent the user from deleting the delay after the normal window expires, thereby missing the end of the window.

## Partition "GOTO" Commands

Each keypad is assigned a default partition for display purposes, and will show only that partition's information. To see information for another partition, or perform system functions in another partition, use the GOTO command (**[User Code] + [*] +partition number 0-8**). The keypad will remain in the new partition until directed to go to another partition, or until 120 seconds has elapsed with no keypad activity. To return to your home partition, enter **[*] + Partition number 0**.

You must program data field 2*18 to enable the GOTO function. This is a partition-specific field that must be set for each partition the user wants to access from another partition's keypad

## Viewing Capabilities of a User

The keypad will display the partitions that a user is authorized for, the user number, and the authority level for all partitions authorized. Enter **[User Code] + [*] + [*]**. The user's capabilities in each authorized partition will typically be displayed as follows:

| |
|---|
| Part. 1 A0* WHSE |
| User 01 Auth.=1G. |

The user's Open/Close report capability is shown by the dot following the authority level. If Open/Close is not enabled for a user, the dot will not appear.

## Viewing Zone Descriptors

The Alpha Keypads can display all programmed descriptors, which is useful to the installer when checking entries, and can be helpful to the user when there is a need to identify zones. ***To display descriptors, the system must be disarmed and ready to arm.*** Press and hold the READY key until the built-in instructions for that key appear, then release the key. The zone descriptors will appear one at a time, for about 2-3 seconds each. For faster viewing, press the READY key to display the next descriptor in numerical order, and so on. When all descriptors have been displayed, the control will exit Display Mode. Enter the Security Code and press the OFF key to exit Display Mode before all descriptors have been displayed.

## Viewing Downloaded Messages

Users may occasionally receive a message from their installation company displayed on an alpha keypad. When this occurs, the keypad will display "Message. Press 0 for 5 secs." Instruct the user to press and hold the 0 key to display the central station's message. Note that the system must be in the READY state to view these messages.

## Using the Built-in User's Manual

An abbreviated User's Manual is stored in the system's memory, and can be particularly useful to the end user if the printed User's Manual is not conveniently accessible when the user needs to perform a seldom-used and unfamiliar system procedure. The Built-in User's Guide is displayed by simply pressing any of the function keys (e.g., OFF, AWAY, STAY, MAXIMUM, BYPASS, INSTANT, CODE, TEST, READY, #, and CHIME) for approximately 5 seconds and then releasing it. Abbreviated instructions relative to the key that has been pressed will then be displayed (2 lines of text are displayed at a time). This function operates in either the armed or the disarmed state.

## Panic Keys

There are three panic key pairs (shown below) that, if programmed, can be used to manually initiate alarms and send a report to the central station. Each key pair can be individually programmed for 24 Hour Silent, Audible or Auxiliary (Emergency) responses, as well as Fire. The panic function is activated when the appropriate key pair is pressed at the same time.

The panic functions are identified by the system as follows:

| PANIC | Zone Number |
|---|---|
| * + 1 | 995 |
| # + 3 | 996 |
| * + # | 999 |

For alpha keypads, these panic keys can also be programmed with an alpha descriptor.

For the panic functions to be of practical value, the system must be connected to a central station.

## Speed Key [D] (Macros)

The system supports up to 32 Speed Key (macro) commands. A Speed Key command is a series of keystrokes stored in the system memory and activated when a programmed lettered key is pressed. Each Speed Key command can include 32 keystrokes. Typical Speed Key functions include:

- Arming sequences that involve first bypassing certain zones before arming.
- Seldom-used but repeatable sequences.
- Relay activation sequences.

Lettered keys A-B-C can be assigned a specific Speed Key function by entering a Speed Key number (1-32) in field 1*26.

### Programming Speed Key Sequence

To program a macro, enter your **[User Code] + [#] + [D]**. The following appears:

```
ENTER SPEED KEY #
01-32          00=QUIT
```

Enter the 2-digit Speed Key number (01-32) being defined and press [*]. Enter up to 32 keystrokes. A Speed Key sequence can include different commands. Press the "D" key to separate different commands.

For example, you may want to perform the following sequence:

| Desired function | Keystrokes |
|---|---|
| GOTO partition 2 | Enter *2 |
| Bypass Zones 10 & 11 | Press bypass [6], then the zone numbers 010 & 011 |
| Arm in Maximum Mode | Press maximum [4] key |
| Return to Partition 1 | Enter *1 |

To program that Speed Key sequence, type the following :

*2[D] 6010011[D] 4[D] *1[D][D]

Note that the "D" key is pressed after each command. Press "D" twice to complete the entry and exit.

When defining Speed Key sequences, do not use the [#] key to represent Quick Arming. The system uses the code entered in response to the prompt to initiate commands in a Speed Key sequence, so the quick arm key is unnecessary. The system interprets the use of the [#] key in a Speed Key sequence as its designated function only (e.g. #2 is not interpreted as "Arm-AWAY," but rather as "Enter House ID Sniffer Mode").

### Executing Speed Key Sequence

To execute a Speed Key sequence, do the following:

If a lettered key, A-B-C, has been assigned as a Speed Key, press the appropriate key. If a user code is required for any part of the Speed Key sequence, the following prompt appears. Otherwise, the Speed Key sequence automatically begins.

| ENTER USER CODE<br>✳✳✳✳ |
|---|

Enter your user code. The programmed Speed Key sequence will begin automatically.

To activate a Speed Key not assigned to the A-B-C keys, press and hold down the [D] key for 2 seconds until the following prompt appears:

| ENTER SPEED KEY #<br>01-32 00=QUIT |
|---|

Enter the desired Speed Key number.

If a user code is required for any part of the Speed Key sequence, the following prompt appears. Otherwise, the Speed Key sequence automatically begins.

| ENTER USER CODE<br>✳✳✳✳ |
|---|

Enter your user code. The programmed Speed Key sequence will begin automatically.

The system will apply the user code's Global Arming capabilities if the macro executes any arming or disarming commands.

## Manual Relay Activation Mode (#70 Mode)

The system allows users to manually activate relays by keypad command using either the keypad or a telephone keypad (if VIP Module is used). The user will be prompted (either by keypad alpha display or telephone voice module).

To activate relays from a keypad, enter 4-digit **[Security Code] + [#] +70.**

To activate relays using a telephone and VIP Module, first dial the 2-digit phone access code. When the system acknowledges the access, enter 4-digit **[Security Code] + [#] + 70**. The following prompts/voice responses will begin.

| ENTER DEVICE NO.<br>00=QUIT 01 | **Voice:** "ENTER DEVICE CODE NOW" |
|---|---|
| | Enter the 2-digit number of the relay to be activated. |
| nn DEVICE IS OFF<br>HIT 0=OFF , 1=ON | **Voice:** "'*VOICE DESCRIPTOR*' DEVICE 'NN' ON/OFF. FOR '*VOICE DESCRIPTOR*' ON, ENTER 1; FOR '*VOICE DESCRIPTOR*' OFF ENTER 0" |
| | Press **0** or **1** to turn the device off or on respectively.<br>'NN' represents the 2-digit relay number and '*VOICE DESCRIPTOR*' is the relay voice descriptor programmed by the installer (see *Relay Voice Descriptors* in the *#93 Menu Mode*). |

| | |
|---|---|
| nn DEVICE IS OFF<br>HIT THE "*" KEY | **Voice:** "'*VOICE DESCRIPTOR*' DEVICE 'NN' ON/OFF. TO EXIT, ENTER 00 NOW" |

From a keypad, press [*] to continue. The ENTER DEVICE NO. prompt will appear.

From a telephone keypad, enter **00** to exit, or enter the next relay number to be programmed. The current on/off state of that relay will be annunciated as described above. Alternatively, if 6 seconds elapses with no key depression, the voice module will annunciate the "ENTER DEVICE CODE NOW" message.

A relay may be designated as restricted to prevent inadvertent activation/deactivation by users. Only the Installer Code can override this restriction in *Output Programming* in the *#93 Menu Mode Programming*

## Instant Activation Mode (#77 Mode)

The #77 Instant Activation Mode is used to activate outputs, bypass zones, etc. immediately upon exiting the #77 Mode. The actions that may be activated by the operator are relay commands, arm/disarm commands, zone bypassing commands, and open/close access conditions.

1. **Enter [User Code] + [#77].**
2. **Enter the code for the desired action and action specifier.** The action codes are the events that are to take place when either the system exits the #77 Mode or the scheduled time is reached, depending on the action selected. 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.

   Refer to *Time Driven Events* in the *Scheduling Options* section for a listing of the "Action Codes" (desired actions) and "Action Specifiers." Note that these codes are independent of the actions programmed during the *Output Programming* in the *#93 Menu Mode*.

**NOTES:**

- Only the Installer and Master levels user codes may perform the Instant Activation Mode.
- When performing an arm or disarm, the user must be assigned to the partition being activated.

# Testing The System

### In This Section



## Battery Test

When AC power is present, the VISTA-128B runs a brief battery test every 60 seconds to determine if the battery connected, and runs an extended battery test every 4 hours to check the battery's condition. If the VISTA-128B finds the battery voltage is low (less than approximately 11.5V) during one of these tests, it displays "SYSTEM LOBAT" on the keypad and a rapid Keypad beeping sound. It also sends a Low Battery report to the central station (if programmed). Clear the keypad by entering any security code + OFF. A Restore report is sent to the central station after a subsequent test indicates the problem has been corrected.

## Dialer Test

The VISTA-128B may be programmed to automatically transmit test reports to a central station at intervals ranging from once per hour to once per 999 hours (field *27). UL requires that a test report be transmitted at least once every 24 hours. The VISTA-128B can be programmed to send the first report at any time of the day, or on any day of the week after power-up (field *83).

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

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 only be activated by the installer, a master user or manager 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 activated, the system will sound burglary bells (or any bell having a non-zero response type in each bell's supervisory zone) for 3 seconds. The system will send a Start of Walk-Test message to the central station. The keypads will display "Burg Walk Test in Progress" and will sound 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 3 beeps from the keypad. Walk in front of any motion detectors. Listen for three beeps when the detector senses movement. The keypad will display the zone number and alpha descriptor while a door or window remains open or while a detector remains activated. The system automatically issues a Zone 8 Glassbreak Detector Power Reset about 10 seconds after it finds a fault on this zone, to allow faulted detectors to be reset.

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

## Armed Burglary System Test

- Alarm messages will be sent to the central station during the following 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, do the following:

| Step | Action |
|---|---|
| 1 | Arm the system and fault one or more zones. Silence alarm sounder(s) each time by entering the code and pressing OFF. Check that entry/exit delay zones provide the assigned delay times. |
| 2 | Check the keypad-initiated alarms, if programmed, by pressing the panic keys (* and #, 1 and *, and/or 3 and #). If the system has been programmed for audible emergency, the keypad will emit a loud, steady alarm sound. The word ALARM and a descriptor "999" will be displayed for * and #. If 1 and * are pressed, a "995" will be displayed; if 3 and # are pressed, a "996" will be displayed. Silence the alarm by entering the security code and pressing OFF. If the system has been programmed for silent panic, there will be no audible alarms or displays. A report will be sent to the central station, however. |
| 3 | Notify the central station that all tests are finished, and verify results with them. |

## Testing Wireless Zones

### Transmitter ID Sniffer Mode

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

To enter the Transmitter ID Sniffer Mode, perform the following steps:

| Step | Action |
|---|---|
| 1 | Enter **[Installer Code] + [#] [3]**. The keypad will display 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 will **disappear** from the display. |
| 3 | To exit, enter the **[Installer Code] + [1]** OFF. |

A transmitter not "enrolled" will not turn off its zone number.

### Go/No Go Test Mode

Before mounting transmitters permanently, conduct Go/No Go Tests to verify adequate signal strength and reorient or relocate transmitters if necessary.

Since the wireless receiver gain is reduced, checking in this mode assists in determining good mounting locations for the transmitters, 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.

- For multi-partition systems, make sure all partitions are disarmed before entering this mode.
- Do not conduct this test with your hand wrapped around the transmitter, as this will cause inaccurate results.

To enter the Go/NoGo Test, perform the following steps:

| Step | Action |
|---|---|
| 1 | Enter **[Installer Code] + [5]** TEST. |
| 2 | Once transmitters are placed in their desired locations and the approximate length of wire to be run to sensors is connected to the transmitter's screw terminals, fault each transmitter.<br>• If a single receiver is used, the keypad will beep three times to indicate signal reception. If two receivers are used, the keypad will beep 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 (which is desirable for redundant configurations).<br>• 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. |
| 3 | Mount the transmitter according to the instructions provided with the transmitter. |
| 4 | Exit the mode by entering **[Installer Code] + [1]** OFF. |

## Trouble Conditions

### Supervisory Messages

- A display of “SUPV” accompanied by a zone number (001-128) and an alpha descriptor (if programmed) indicates that a fire supervisory condition exists on that zone. This means that the operation of the fire alarm system may be compromised.

### Check or Trouble Messages

- A display of "CHECK" or "TRBL" (as per field 1*07) accompanied by a zone number (001-128) and an alpha descriptor indicates that a problem exists with that zone. 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" accompanied by a numeric display of "6XX," where XX = 01-32, indicates a trouble on a 4204CF Supervised Bell Output (corresponding relay number 01-32).

- "CHECK" accompanied by a numeric display of "8XX," where XX = 00-31, indicates a trouble on a peripheral device (connected to the panel's keypad terminals) of the corresponding device address (00-31).
- "CHECK" accompanied by a numeric display of "9XX," where XX = 00-99, indicates that a system trouble exists (dialers, bell outputs, ground fault, etc.). See the *Zone Index/Zone Type Defaults* section.

If the problem has been corrected, key an OFF sequence (Security Code plus OFF) twice to clear the display.

### Other System Messages

- "COMM. FAILURE" at the keypad indicates that a failure occurred in the telephone communication portion of your system.
- "LO BAT" and a zone descriptor, accompanied by a once-per-minute beep at the keypad, indicates that a low battery condition exists in the wireless transmitter displayed. Pressing any key will silence the audible warning sound.
- "SYSTEM LO BAT" at the keypad indicates that a low battery condition exists with the system's backup battery.
- "RCVR SET UP ERROR" at the keypad 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" at the keypad indicates that the control is on-line with a remote computer.

### System Off-Normal Report

If programmed, a unique Off-Normal report will be generated instead of the periodic test report if any of the following conditions are present at the time of the report:

- Fire trouble on any zone (zone response types 9)
- Unrestored fire alarm on any zone
- Fault on LORRA "XMIT OK" signal (if enabled)
- LORRA trigger bypassed
- AC failure
- Low system battery
- Keypad supervision fault

This report will be sent as follows:

Contact ID: Code 608

High Speed: Channel 3 of system report used (channel 9=6)

Low Speed: Digits programmed in System Group #4 report codes (*Report Code Programming* in the *#93 Menu Mode*).

### Power Failure

If the POWER indicator is off, and the message "AC LOSS" is displayed, the keypad 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.

## 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's Manual 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.

## 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.

### 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.
- Be sure 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 ADEMCO customer number and/or company name.

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

You may contact Technical Support via Toll-Free Fax. Please include your return fax number. You will receive a reply within 24 hours. You may also contact Technical Support via modem to ATLIS-BBS, Tech Support's Electronic Bulletin Board System. Replies are posted within 24 hours.

| | |
|---|---|
| *Technical Support:* | 1-800-645-7492 (8 a.m.-8 p.m. E.S.T.) |
| *Technical Support Fax Number:* | 1-800-447-5086 |
| *ATLIS-BB Electronic Bulletin Board System:* | 1-516-496-3980 |
| *(1200 - 9600 Baud, 8 Data Bits, 1 Start/Stop Bit, No Parity)* | |
| *ATLIS-FAX FAXBACK Automated Fax Retrieval System:* | 1-800-573-0153 or |
| | 1-516-921-6704 / ext. 1667 |
| *World Wide Web Address:* | HTTP://WWW.ADEMCO.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-128B) 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.

## UL609 Grade A Local Mercantile Premises/Local Mercantile Safe & Vault

- Use the VISTA-128B.
- All zones must be configured for EOLR supervision (*41=0). Wireless sensors may not be used. If 4190WH RPMs are used, set field *24 to "0" to enable tamper detection.
- Attach a door tamper switch (supplied) to the VISTA-128B cabinet backbox. For safe and vault installations, a shock sensor (not supplied) must also be attached to the backbox. (Also see *Mounting the Cabinet* in the *Installing the Control* section)
- Wire an ADEMCO AB12 Grade A Bell/Box to the bell output. Bell wires must be run in conduit. Program the bell output for 16 or longer timeout and for confirmation of arming ding. (Also see the *External Sounders* section)
- Wire the VISTA-128B tamper switch and AB12 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 Police Station Connected Burglar Alarm

Follow the instructions for UL609 local installations given above.

### For Grade A Service:

- You may use the VISTA-128B dialer alone, or the 7720 Long Range Radio alone.
- When using the dialer, program it to send Burglary Alarm, Low Battery and Communicator Test reports. Field *27 must be set to "024" (or less) so that test reports are sent at least once every 24 hours.
- If using the 7720, connect it to the VISTA-128B burglary/audible panic alarm trigger.

**For Grade AA Service:**

- You must use a 7920SE Long Range Radio.
- Connect the 7920SE to the VISTA-128B burglary/audible panic alarm trigger.

## UL611/UL1610 Central Station Burglary Alarm

Follow the instructions for UL609 Local installations given above.

**For Grade A Service:**

- You must use the VISTA-128B's dialer with a 7720 Long Range Radio.
- Connect the control's burglary/audible panic alarm trigger (on J7 header) and the 659EN's phone line monitor output to the 7720. The 7720 will send a report to the central station when a telephone line fault condition is detected.
- Also connect the 7720's radio fault output to one of the VISTA-128B's 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 radio faults.
- Program the control's dialer to send Burglary Alarm, Trouble, Opening/Closing,, and Low Battery reports.

**For Grade AA Service:**

- Follow the instructions for Grade A service, except use the 7920SE in place of the 7720.

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

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

The VISTA-128B 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)
- Use 14AH battery (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 which has been approved by UL and CSFM for fire zone usage). Both batteries will fit inside the panel's cabinet.

**"FEDERAL COMMUNICATIONS COMMISSION (FCC) STATEMENT"**

This equipment has been tested to FCC requirements and has been found acceptable for use. The FCC requires the following statement for your information:

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for a Class B computing device in accordance with the specifications in Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause 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:

- If using an indoor antenna, have a quality outdoor antenna installed.
- Reorient the receiving antenna until interference is reduced or eliminated.
- Move the receiver away from the control/communicator.
- Move the antenna leads away from any wire runs to the control/communicator.
- Plug the control/communicator into a different outlet so that it and the receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions.

The user or installer may find the following booklet prepared by the Federal Communications Commission helpful:

"Interference Handbook"

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402.

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.

**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 they have 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 which 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 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 DEPARTMENT OF COMMUNICATIONS**
**(DOC) STATEMENT**

**NOTICE**

The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. 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. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of certified connector assembly (telephone extension cord). 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 made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause 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:** User should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

**AVIS**

L'étiquette du ministère des Communications du Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme à certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. 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'entreprise locale de télécommunications. Le matériel doit également être installé en suivant une méthode acceptée de raccordement. Dans certains cas, les fils intérieurs de l'entreprise utilisés pour un service individuel à la ligne unique peuvent être prolongés au moyen d'un dispositif homologué de raccordement (cordon prolongateur téléphonique interne). L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empèchet pas la dégradation du service dans certaines situations. Actuellement, les entreprises de télécommunications ne permettent pas que l'on raccorde leur matériel aux prises d'abonnés, sauf dans les cas precis prévus par les tarifs particuliers de ces entreprises.

Les réparations du matériel homologué doivent être effectuées pas un centre d'entretien canadien autorisé désigné par le fournisseur. La compagnie de télécommunications peut demander à l'utilisateur de 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 en terre de la source d'énergie électrique, des lignes téléphoniques de réseau de conduites d'eau s'il y en a, soient 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 recours à un service d'inspection des installations électriques, ou à un électricien, selon le cas.

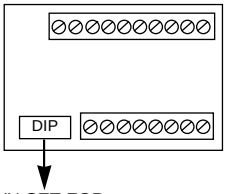
L'indice de charge (IC) assigné à chaque dispositif terminal pour éviter toute surcharge indique le pourcentage de la charge totale qui peut être raccordé à un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit bouclé peut être constituée de n'importe quelle combinaison de dispositifs, pourvu que la somme des indices de charge de l'ensemble des dispositifs ne dépasse pas 100.

*A P P E N D I X  B*

# *DIP Switch Tables*

# DIP SWITCH TABLES FOR ADDRESSABLE POLLING LOOP DEVICES

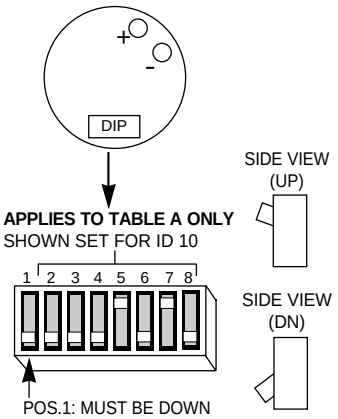
## 4208 ZONE EXPANDER



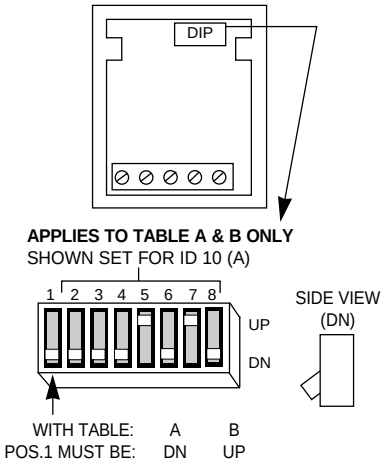

POS.1: LOOPS 1 & 2
RESPONSE TIME:

| W/TABLE | FAST | SLOW |
|---|---|---|
| A | UP | DN |
| B | DN | UP |

## 4192D/4192SDT/4192CP SMOKE DETECTORS




## 4190WH ZONE EXPANDER




THIS TABLE FOR DIPS WITH WORD "DN" ("—" = DN) **A**

| DEVICE ID | DIP SWITCH POSITION | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| 10-16 | — | — | — | UP |
| 17-24 | — | — | UP | — |
| 25-32 | — | — | UP | UP |
| 33-40 | — | UP | — | — |
| 41-48 | — | UP | — | UP |
| 49-56 | — | UP | UP | — |
| 57-64 | — | UP | UP | UP |

THIS TABLE FOR DIPS WITH WORD "UP" ("—" = DN) **B**

| DEVICE ID | DIP SWITCH POSITION | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| 10-16 | UP | UP | UP | — |
| 17-24 | UP | UP | — | UP |
| 25-32 | UP | UP | — | — |
| 33-40 | UP | — | UP | UP |
| 41-48 | UP | — | UP | — |
| 49-56 | UP | — | — | UP |
| 57-64 | UP | — | — | — |

THIS TABLE FOR DIPS WITH WORD "DN" ("–" = DN) **A**

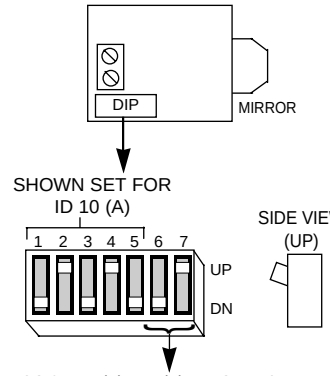
| DEVICE ID | DIP SWITCH POSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | – | – | – | UP | – | UP | – |
| 11 | – | – | – | UP | – | UP | UP |
| 12 | – | – | – | UP | UP | – | – |
| 13 | – | – | – | UP | UP | – | UP |
| 14 | – | – | – | UP | UP | UP | – |
| 15 | – | – | – | UP | UP | UP | UP |
| 16 | – | – | UP | – | – | – | – |
| 17 | – | – | UP | – | – | – | UP |
| 18 | – | – | UP | – | – | UP | – |
| 19 | – | – | UP | – | – | UP | UP |
| 20 | – | – | UP | – | UP | – | – |
| 21 | – | – | UP | – | UP | – | UP |
| 22 | – | – | UP | – | UP | UP | – |
| 23 | – | – | UP | – | UP | UP | UP |
| 24 | – | – | UP | UP | – | – | – |
| 25 | – | – | UP | UP | – | – | UP |
| 26 | – | – | UP | UP | – | UP | – |
| 27 | – | – | UP | UP | – | UP | UP |
| 28 | – | – | UP | UP | UP | – | – |
| 29 | – | – | UP | UP | UP | – | UP |
| 30 | – | – | UP | UP | UP | UP | – |
| 31 | – | – | UP | UP | UP | UP | UP |
| 32 | – | UP | – | – | – | – | – |
| 33 | – | UP | – | – | – | – | UP |
| 34 | – | UP | – | – | – | UP | – |
| 35 | – | UP | – | – | – | UP | UP |
| 36 | – | UP | – | – | UP | – | – |
| 37 | – | UP | – | – | UP | – | UP |
| 38 | – | UP | – | – | UP | UP | – |
| 39 | – | UP | – | – | UP | UP | UP |
| 40 | – | UP | – | UP | – | – | – |
| 41 | – | UP | – | UP | – | – | UP |
| 42 | – | UP | – | UP | – | UP | – |
| 43 | – | UP | – | UP | – | UP | UP |
| 44 | – | UP | – | UP | UP | – | – |
| 45 | – | UP | – | UP | UP | – | UP |
| 46 | – | UP | – | UP | UP | UP | – |
| 47 | – | UP | – | UP | UP | UP | UP |
| 48 | – | UP | UP | – | – | – | – |
| 49 | – | UP | UP | – | – | – | UP |
| 50 | – | UP | UP | – | – | UP | – |
| 51 | – | UP | UP | – | – | UP | UP |
| 52 | – | UP | UP | – | UP | – | – |
| 53 | – | UP | UP | – | UP | – | UP |
| 54 | – | UP | UP | – | UP | UP | – |
| 55 | – | UP | UP | – | UP | UP | UP |
| 56 | – | UP | UP | UP | – | – | – |
| 57 | – | UP | UP | UP | – | – | UP |
| 58 | – | UP | UP | UP | – | UP | – |
| 59 | – | UP | UP | UP | – | UP | UP |
| 60 | – | UP | UP | UP | UP | – | – |
| 61 | – | UP | UP | UP | UP | – | UP |
| 62 | – | UP | UP | UP | UP | UP | – |
| 63 | – | UP | UP | UP | UP | UP | UP |
| 64 | UP | – | – | – | – | – | – |
| 65 | UP | – | – | – | – | – | UP |
| 66 | UP | – | – | – | – | UP | – |
| 67 | UP | – | – | – | – | UP | UP |
| 68 | UP | – | – | – | UP | – | – |
| 69 | UP | – | – | – | UP | – | UP |
| 70 | UP | – | – | – | UP | UP | – |
| 71 | UP | – | – | – | UP | UP | UP |
| 72 | UP | – | – | UP | – | – | – |
| 73 | UP | – | – | UP | – | – | UP |
| 74 | UP | – | – | UP | – | UP | – |
| 75 | UP | – | – | UP | – | UP | UP |
| 76 | UP | – | – | UP | UP | – | – |
| 77 | UP | – | – | UP | UP | – | UP |
| 78 | UP | – | – | UP | UP | UP | – |
| 79 | UP | – | – | UP | UP | UP | UP |
| 80 | UP | – | UP | – | – | – | – |
| 81 | UP | – | UP | – | – | – | UP |
| 82 | UP | – | UP | – | – | UP | – |
| 83 | UP | – | UP | – | – | UP | UP |
| 84 | UP | – | UP | – | UP | – | – |
| 85 | UP | – | UP | – | UP | – | UP |
| 86 | UP | – | UP | – | UP | UP | – |
| 87 | UP | – | UP | – | UP | UP | UP |
| 88 | UP | – | UP | UP | – | – | – |
| 89 | UP | – | UP | UP | – | – | UP |
| BIT VALUE: | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

THIS TABLE FOR DIPS WITH WORD "UP" ("–" = DN) **B**

| DEVICE ID | DIP SWITCH POSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | UP | UP | UP | – | UP | – | UP |
| 11 | UP | UP | UP | – | UP | – | – |
| 12 | UP | UP | UP | – | – | UP | UP |
| 13 | UP | UP | UP | – | – | UP | – |
| 14 | UP | UP | UP | – | – | – | UP |
| 15 | UP | UP | UP | – | – | – | – |
| 16 | UP | UP | – | UP | UP | UP | UP |
| 17 | UP | UP | – | UP | UP | UP | – |
| 18 | UP | UP | – | UP | UP | – | UP |
| 19 | UP | UP | – | UP | UP | – | – |
| 20 | UP | UP | – | UP | – | UP | UP |
| 21 | UP | UP | – | UP | – | UP | – |
| 22 | UP | UP | – | UP | – | – | UP |
| 23 | UP | UP | – | UP | – | – | – |
| 24 | UP | UP | – | – | UP | UP | UP |
| 25 | UP | UP | – | – | UP | UP | – |
| 26 | UP | UP | – | – | UP | – | UP |
| 27 | UP | UP | – | – | UP | – | – |
| 28 | UP | UP | – | – | – | UP | UP |
| 29 | UP | UP | – | – | – | UP | – |
| 30 | UP | UP | – | – | – | – | UP |
| 31 | UP | UP | – | – | – | – | – |
| 32 | UP | – | UP | UP | UP | UP | UP |
| 33 | UP | – | UP | UP | UP | UP | – |
| 34 | UP | – | UP | UP | UP | – | UP |
| 35 | UP | – | UP | UP | UP | – | – |
| 36 | UP | – | UP | UP | – | UP | UP |
| 37 | UP | – | UP | UP | – | UP | – |
| 38 | UP | – | UP | UP | – | – | UP |
| 39 | UP | – | UP | UP | – | – | – |
| 40 | UP | – | UP | – | UP | UP | UP |
| 41 | UP | – | UP | – | UP | UP | – |
| 42 | UP | – | UP | – | UP | – | UP |
| 43 | UP | – | UP | – | UP | – | – |
| 44 | UP | – | UP | – | – | UP | UP |
| 45 | UP | – | UP | – | – | UP | – |
| 46 | UP | – | UP | – | – | – | UP |
| 47 | UP | – | UP | – | – | – | – |
| 48 | UP | – | – | UP | UP | UP | UP |
| 49 | UP | – | – | UP | UP | UP | – |
| 50 | UP | – | – | UP | UP | – | UP |
| 51 | UP | – | – | UP | UP | – | – |
| 52 | UP | – | – | UP | – | UP | UP |
| 53 | UP | – | – | UP | – | UP | – |
| 54 | UP | – | – | UP | – | – | UP |
| 55 | UP | – | – | UP | – | – | – |
| 56 | UP | – | – | – | UP | UP | UP |
| 57 | UP | – | – | – | UP | UP | – |
| 58 | UP | – | – | – | UP | – | UP |
| 59 | UP | – | – | – | UP | – | – |
| 60 | UP | – | – | – | – | UP | UP |
| 61 | UP | – | – | – | – | UP | – |
| 62 | UP | – | – | – | – | – | UP |
| 63 | UP | – | – | – | – | – | – |
| 64 | – | UP | UP | UP | UP | UP | UP |
| 65 | – | UP | UP | UP | UP | UP | – |
| 66 | – | UP | UP | UP | UP | – | UP |
| 67 | – | UP | UP | UP | UP | – | – |
| 68 | – | UP | UP | UP | – | UP | UP |
| 69 | – | UP | UP | UP | – | UP | – |
| 70 | – | UP | UP | UP | – | – | UP |
| 71 | – | UP | UP | UP | – | – | – |
| 72 | – | UP | UP | – | UP | UP | UP |
| 73 | – | UP | UP | – | UP | UP | – |
| 74 | – | UP | UP | – | UP | – | UP |
| 75 | – | UP | UP | – | UP | – | – |
| 76 | – | UP | UP | – | – | UP | UP |
| 77 | – | UP | UP | – | – | UP | – |
| 78 | – | UP | UP | – | – | – | UP |
| 79 | – | UP | UP | – | – | – | – |
| 80 | – | UP | – | UP | UP | UP | UP |
| 81 | – | UP | – | UP | UP | UP | – |
| 82 | – | UP | – | UP | UP | – | UP |
| 83 | – | UP | – | UP | UP | – | – |
| 84 | – | UP | – | UP | – | UP | UP |
| 85 | – | UP | – | UP | – | UP | – |
| 86 | – | UP | – | UP | – | – | UP |
| 87 | – | UP | – | UP | – | – | – |
| 88 | – | UP | – | – | UP | UP | UP |
| 89 | – | UP | – | – | UP | UP | – |
| BIT VALUE: | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

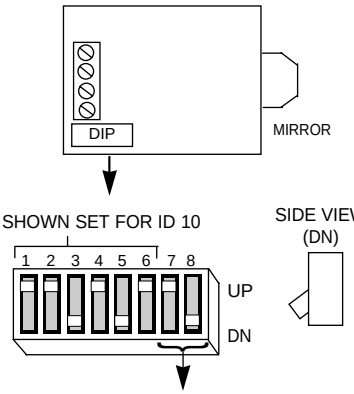
# DIP SWITCH TABLES FOR POLLING LOOP DEVICES

## 4275 PIR



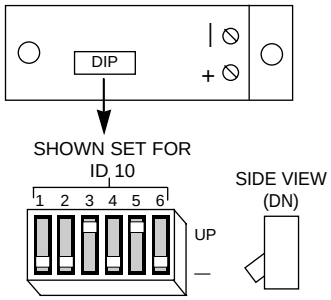

POS 6: UP (A), DN (B) = INST. MODE
DN (A), UP (B) = PULSE COUNT
POS. 7: UP (A), DN (B) = WALK TEST
DN (A), UP (B) = W/T DISABLE

## 4278 PIR




POS 7: UP = NORMAL MODE
DN = INSTANT MODE
POS. 8: UP = W/T DISABLE
DN = WALK TEST

## 4194 REED CONTACT (SURFACE MOUNT)




THIS TABLE FOR DIPS WITH WORD "DN" **A**

| DEVICE ID | DIP SWITCH POSITION | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 10 | — | UP | — | UP | — |
| 11 | — | UP | — | UP | UP |
| 12 | — | UP | UP | — | — |
| 13 | — | UP | UP | — | UP |
| 14 | — | UP | UP | UP | — |
| 15 | — | UP | UP | UP | UP |
| 16 | UP | — | — | — | — |
| 17 | UP | — | — | — | UP |
| 18 | UP | — | — | UP | — |
| 19 | UP | — | — | UP | UP |
| 20 | UP | — | UP | — | — |
| 21 | UP | — | UP | — | UP |
| 22 | UP | — | UP | UP | — |
| 23 | UP | — | UP | UP | UP |
| 24 | UP | UP | — | — | — |
| 25 | UP | UP | — | — | UP |
| 26 | UP | UP | — | UP | — |
| 27 | UP | UP | — | UP | UP |
| 28 | UP | UP | UP | — | — |
| 29 | UP | UP | UP | — | UP |
| 30 | UP | UP | UP | UP | — |
| 31 | UP | UP | UP | UP | UP |

THIS TABLE FOR DIPS WITH WORD "UP" **B**

| DEVICE ID | DIP SWITCH POSITION | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 10 | UP | — | UP | — | UP |
| 11 | UP | — | UP | — | — |
| 12 | UP | — | — | UP | UP |
| 13 | UP | — | — | UP | — |
| 14 | UP | — | — | — | UP |
| 15 | UP | — | — | — | — |
| 16 | — | UP | UP | UP | UP |
| 17 | — | UP | UP | UP | — |
| 18 | — | UP | UP | — | UP |
| 19 | — | UP | UP | — | — |
| 20 | — | UP | — | UP | UP |
| 21 | — | UP | — | UP | — |
| 22 | — | UP | — | — | UP |
| 23 | — | UP | — | — | — |
| 24 | — | — | UP | UP | UP |
| 25 | — | — | UP | UP | — |
| 26 | — | — | UP | — | UP |
| 27 | — | — | UP | — | — |
| 28 | — | — | — | UP | UP |
| 29 | — | — | — | UP | — |
| 30 | — | — | — | — | UP |
| 31 | — | — | — | — | — |
| BIT VALUE: | 16 | 8 | 4 | 2 | 1 |

| DEVICE ID | DIP SWITCH POSITION | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 10 | UP | UP | — | UP | — | UP |
| 11 | UP | UP | — | UP | — | — |
| 12 | UP | UP | — | — | UP | UP |
| 13 | UP | UP | — | — | UP | — |
| 14 | UP | UP | — | — | — | UP |
| 15 | UP | UP | — | — | — | — |
| 16 | UP | — | UP | UP | UP | UP |
| 17 | UP | — | UP | UP | UP | — |
| 18 | UP | — | UP | UP | — | UP |
| 19 | UP | — | UP | UP | — | — |
| 20 | UP | — | UP | — | UP | UP |
| 21 | UP | — | UP | — | UP | — |
| 22 | UP | — | UP | — | — | UP |
| 23 | UP | — | UP | — | — | — |
| 24 | UP | — | — | UP | UP | UP |
| 25 | UP | — | — | UP | UP | — |
| 26 | UP | — | — | UP | — | UP |
| 27 | UP | — | — | UP | — | — |
| 28 | UP | — | — | — | UP | UP |
| 29 | UP | — | — | — | UP | — |
| 30 | UP | — | — | — | — | UP |
| 31 | UP | — | — | — | — | — |
| 32 | — | UP | UP | UP | UP | UP |
| 33 | — | UP | UP | UP | UP | — |
| 34 | — | UP | UP | UP | — | UP |
| 35 | — | UP | UP | UP | — | — |
| 36 | — | UP | UP | — | UP | UP |
| 37 | — | UP | UP | — | UP | — |
| 38 | — | UP | UP | — | — | UP |
| 39 | — | UP | UP | — | — | — |
| 40 | — | UP | — | UP | UP | UP |
| 41 | — | UP | — | UP | UP | — |
| 42 | — | UP | — | UP | — | UP |
| 43 | — | UP | — | UP | — | — |
| 44 | — | UP | — | — | UP | UP |
| 45 | — | UP | — | — | UP | — |
| 46 | — | UP | — | — | — | UP |
| 47 | — | UP | — | — | — | — |
| 48 | — | — | UP | UP | UP | UP |
| 49 | — | — | UP | UP | UP | — |
| 50 | — | — | UP | UP | — | UP |
| 51 | — | — | UP | UP | — | — |
| 52 | — | — | UP | — | UP | UP |
| 53 | — | — | UP | — | UP | — |
| 54 | — | — | UP | — | — | UP |
| 55 | — | — | UP | — | — | — |
| 56 | — | — | — | UP | UP | UP |
| 57 | — | — | — | UP | UP | — |
| 58 | — | — | — | UP | — | UP |
| 59 | — | — | — | UP | — | — |
| 60 | — | — | — | — | UP | UP |
| 61 | — | — | — | — | UP | — |
| 62 | — | — | — | — | — | UP |
| 63 | — | — | — | — | — | — |
| BIT VALUE: | 32 | 16 | 8 | 4 | 2 | 1 |

| DEVICE ID | DIP SWITCH POSITION | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 10 | — | — | UP | — | UP | — |
| 11 | — | — | UP | — | UP | UP |
| 12 | — | — | UP | UP | — | — |
| 13 | — | — | UP | UP | — | UP |
| 14 | — | — | UP | UP | UP | — |
| 15 | — | — | UP | UP | UP | UP |
| 16 | — | Up | — | — | — | — |
| 17 | — | UP | — | — | — | UP |
| 18 | — | UP | — | — | UP | — |
| 19 | — | UP | — | — | UP | UP |
| 20 | — | UP | — | UP | — | — |
| 21 | — | UP | — | UP | — | UP |
| 22 | — | UP | — | UP | UP | — |
| 23 | — | UP | — | UP | UP | UP |
| 24 | — | UP | UP | — | — | — |
| 25 | — | UP | UP | — | — | UP |
| 26 | — | UP | UP | — | UP | — |
| 27 | — | UP | UP | — | UP | UP |
| 28 | — | UP | UP | UP | — | — |
| 29 | — | UP | UP | UP | — | UP |
| 30 | — | UP | UP | UP | UP | — |
| 31 | — | UP | UP | UP | UP | UP |
| 32 | UP | — | — | — | — | — |
| 33 | UP | — | — | — | — | UP |
| 34 | UP | — | — | — | UP | — |
| 35 | UP | — | — | — | UP | UP |
| 36 | UP | — | — | UP | — | — |
| 37 | UP | — | — | UP | — | UP |
| 38 | UP | — | — | UP | UP | — |
| 39 | UP | — | — | UP | UP | UP |
| 40 | UP | — | UP | — | — | — |
| 41 | UP | — | UP | — | — | UP |
| 42 | UP | — | UP | — | UP | — |
| 43 | UP | — | UP | — | UP | UP |
| 44 | UP | — | UP | UP | — | — |
| 45 | UP | — | UP | UP | — | UP |
| 46 | UP | — | UP | UP | UP | — |
| 47 | UP | — | UP | UP | UP | UP |
| 48 | UP | UP | — | — | — | — |
| 49 | UP | UP | — | — | — | UP |
| 50 | UP | UP | — | — | UP | — |
| 51 | Up | UP | — | — | UP | UP |
| 52 | UP | UP | — | UP | — | — |
| 53 | UP | UP | — | UP | — | UP |
| 54 | UP | UP | — | UP | UP | — |
| 55 | UP | UP | — | UP | UP | UP |
| 56 | UP | UP | UP | — | — | — |
| 57 | UP | UP | UP | — | — | UP |
| 58 | UP | UP | UP | — | UP | — |
| 59 | UP | UP | UP | — | UP | UP |
| 60 | UP | UP | UP | UP | — | — |
| 61 | UP | UP | UP | UP | — | UP |
| 62 | UP | UP | UP | UP | UP | — |
| 63 | UP | UP | UP | UP | UP | UP |
| BIT VALUE: | 32 | 16 | 8 | 4 | 2 | 1 |

# Summary of System Commands

**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)

**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

**Arming Functions**

| | |
|---|---|
| Arming Away | Enter Code + Away [2]. |
| Arming Stay | Enter Code + Stay [3]. |
| Arming Instant | Enter Code + Instant [7]. |
| Arming Maximum | Enter Code + Maximum [4]. |
| Quick Arm | Use # Key Instead Of User Code Followed by Any of the Above Arming Mode Keys. |
| Global Arming | If Enabled for the User, the Keypad Will Display a Prompt. Answer The Prompted Questions |
| Disarming | Enter Code + Off [1]. |
| Bypassing Zones | Enter Code + Bypass [6] + Zone Number. |
| Quick Bypass | To Automatically Bypass All Faulted Zones, Use "Quick Bypass" Method: Enter Code + Bypass + [#]. |
| Chime Mode | Enter Code + Chime [9]. To Turn Chime Mode Off, Enter Code + Chime Again. |
| Partition GOTO | User Code + [*] + Partition Number 0-8. |
| GOTO Home Partition | User Code + [*] + 0. |
| Panics | [*] + 1 Zone 995 (A Key).<br>[*] + [#] Zone 999 (B Key).<br>[#] + 3 Zone 996 (C Key). |
| View Downloaded Messages | Press 0 for 5 Seconds. |
| Display All Zone Descriptors | Press [*] for 5 Seconds. |
| Display User Self Help | Hold Any Key for 5 Seconds |

| | |
|---|---|
| **Programming Commands** | Site Initiated Download = User Code + [#] + 1. |
| | Direct-Wire Download Enable = User Code + [#] + 5. |
| | Enter Program Mode = Installer Code + 8000. |
| | Exit Program Mode = *99 Or *98. |
| **Scheduling Commands** | Programmed Schedule Events = User 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. |
| **Output Device Control** | 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. |
| **Access Control** | 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. |

*APPENDIX D*

# Specifications

## VISTA-128B CONTROL

**Physical:** 14-1/2"W X 18"H X 4.3"D

**Electrical:**

| | |
|---|---|
| Voltage Input: | From ADEMCO No. 1361 Plug-In Transformer (use 1361CN in Canada) or 4300 transformer (for X-10 installations) rated 16.5VAC, 40 VA. |
| Alarm Sounder Output: | 10VDC-13.8VDC, 1.7 amps 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: | ADEMCO High Speed, ADEMCO 4 + 2 Express, ADEMCO Low Speed, ADEMCO Contact ID, Sescoa and Radionics Low Speed |
| Line Seize: | Double Pole |
| Ringer Equivalence: | 0.7B |
| FCC Registration No.: | AC398U-68192-AL-E |

**6139 Remote Keypads**

**Physical:**

| | |
|---|---|
| Width: | 6.25 inches |
| Height: | 4.75 inches |
| Depth: | 1.25 inches |

**Electrical:**

| | |
|---|---|
| Voltage Input: | 12VDC |
| Current Drain: | 100 mA |

**Interface Wiring:**

| | |
|---|---|
| RED: | 12VDC input (+) auxiliary power |
| BLUE: | Not Used |
| GREEN: | Data to control panel |
| YELLOW: | Data from control panel |
| BLACK: | Ground and (-) connection from supplemental power supply. |

# Index



## A

## B



## C



## D

## E



## F



## G



## H



## I



## J



## K

## L



## M



## N



## O



## P

## Q



## R



## S



## T

## U



## V



## W



## 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.

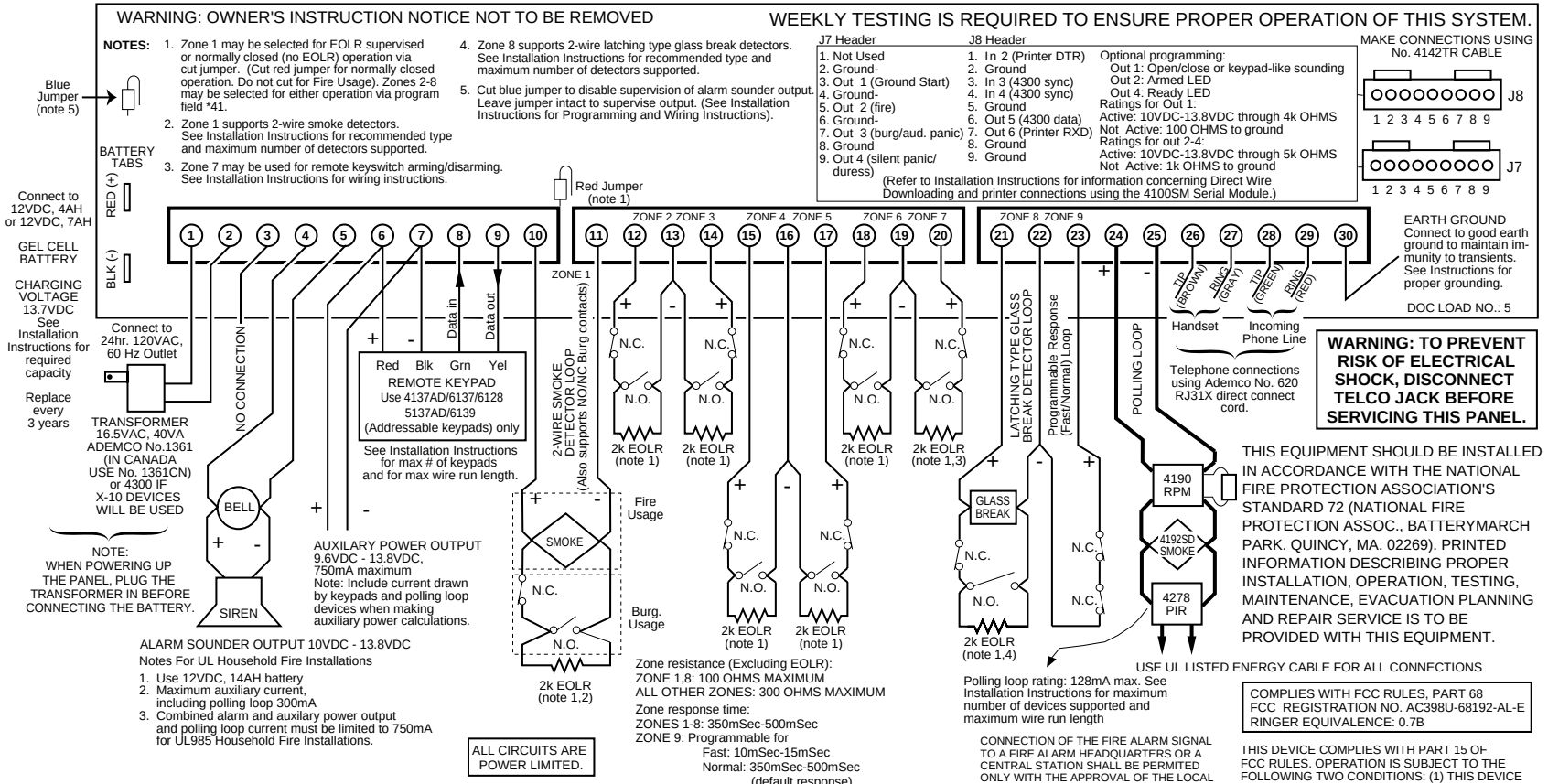
Installing an alarm system may make the owner eligible for a lower insurance rate, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property. We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

## ADEMCO LIMITED WARRANTY

Alarm Device Manufacturing Company, a Division of Pittway Corporation, and its divisions, subsidiaries and affiliates ("Seller"), 165 Eileen Way, Syosset, New York 11791, warrants its products to be in conformance with its own plans and specifications and to be free from defects in materials and workmanship under normal use and service for 24 months from the date stamp control on the product or, for products not having an ADEMCO date stamp, for 12 months from date of original purchase unless the installation instructions or catalog sets forth a shorter period, in which case the shorter period shall apply. Seller's obligation shall be limited to repairing or replacing, at its option, free of charge for materials or labor, any product which is proved not in compliance with Seller's specifications or proves defective in materials or workmanship under normal use and service. Seller shall have no obligation under this Limited Warranty or otherwise if the product is altered or improperly repaired or serviced by anyone other than ADEMCO factory service. For warranty service, return product transportation prepaid, to ADEMCO Factory Service, 170 Michael Drive, Syosset, New York 11791.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. IN NO CASE SHALL SELLER BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, OR UPON ANY OTHER BASIS OF LIABILITY WHATSOEVER, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT.

Seller does not represent that the products it sells may not be compromised or circumvented; that the products will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the products will in all cases provide adequate warning or protection. Customer understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery, fire or other events occurring without providing an alarm, but it is not insurance or a guarantee that such will not occur or that there will be no personal injury or property loss as a result. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. HOWEVER, IF SELLER IS HELD LIABLE, WHETHER DIRECTLY OR INDIRECTLY, FOR ANY LOSS OR DAMAGE ARISING UNDER THIS LIMITED WARRANTY OR OTHERWISE, REGARDLESS OF CAUSE OR ORIGIN, SELLER'S MAXIMUM LIABILITY SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT, WHICH SHALL BE THE COMPLETE AND EXCLUSIVE REMEDY AGAINST SELLER. This warranty replaces any previous warranties and is the only warranty made by Seller on this product. No increase or alteration, written or verbal, of the obligations of this Limited Warranty is authorized.




# VISTA-128B
# SUMMARY OF CONNECTIONS


**165 Eileen Way, Syosset, New York 11791**



**K3271V1 9/00**