

ADEMCO VISTA-120IT

Partitioned Security System With Scheduling

Installation and Setup Guide

This control complies with EN50131

Table of Contents

LIST OF FIGURES	V
CONVENTIONS USED IN THIS MANUAL	VI
SECTION 1: GENERAL DESCRIPTION	1-1
General Description	1-1
New Features	1-1
SECTION 2: PARTITIONING AND PANEL LINKING	2-1
Theory of Partitioning	2-1
Setting Up a Partitioned System	2-1
Common Area Logic	2-1
Master Keypad Setup and Operation	2-4
Panel Linking	2-4
How to Use Panel Linking	2-5
SECTION 3: INSTALLING THE CONTROL	3-1
Mounting the Cabinet	3-1
Installing The Cabinet Lock	3-1
Installing the Control's Circuit Board	3-1
Installing the Keypads	3-2
Installing External Sounders	3-3
Standard Phone Line Connections	3-4
Wiring Devices to Zones 1-9	3-4
Installing Polling Loop Devices	3-7
Wireless (RF) Zone Expansion	3-9
Installing Output Devices	3-12
Open/Close Trigger Setup	3-14
Installing a Remote Keypad Sounder	3-14
Installing a Remote Keypad Switch	3-14
Auxiliary Alarm Signaling Equipment	3-15
Installing the VA8200 Panel Link Module	3-15
Event Log Printer Connections	3-16
Long Range Radio Connected to the ECP	3-17
Installing the 4286 VISTA Interactive Phone (VIP) Module	3-18
Installing a Telephone Line Monitor	3-20
Installing Audio Alarm Verification (AAV)	3-21
Video Alarm Verification (VAV)	3-23
Access Control Using ADEMCO VistaKey	3-24
Access Control Using ADEMCO PassPoint ACS	3-25
Connecting the AC Mains Transformer	3-26
Earth Ground Connections	3-26
Calculating the Battery Size Needed	3-27
Installing The Back-Up Battery	3-27
SECTION 4: PROGRAMMING	4-1
Program Modes	4-1
Entering and Exiting Programming Mode	4-1
Data Field Programming Mode	4-1
#93 Menu Mode Programming	4-2
Zone Index	4-3
Communication Programming Guide	4-4
Zone Response Type Definitions	4-5
Zone Input Type Definitions	4-7
Programming Access Control of an Entry/Exit Point	4-8
Programming for Panel Linking	4-9

Programming for the Video Alarm Verification	4-10
SECTION 5: DATA FIELD DESCRIPTIONS	5-1
About Data Field Programming	5-1
Programming Data Fields	5-1
SECTION 6: SCHEDULING OPTIONS	6-1
Introduction To Scheduling	6-1
Time Period Definitions	6-2
Open/Close Definitions	6-3
Scheduling Menu Mode.....	6-4
Time Periods.....	6-5
Daily Open/Close Schedules	6-5
Holiday Schedules	6-6
Time Driven Events	6-7
Limitation of Access Schedules.....	6-11
Temporary Schedules	6-12
User Scheduling Menu Mode.....	6-13
SECTION 7: DOWNLOADING	7-1
General Information	7-1
Getting On-Line with a Control Panel.....	7-1
On-Line Control Functions.....	7-2
Access Security.....	7-2
Connecting a 4100SM Module for Direct Wire Downloading	7-2
SECTION 8: SETTING THE REAL-TIME CLOCK	8-1
General Information	8-1
Setting the Time and Date	8-1
SECTION 9: SECURITY ACCESS CODES	9-1
General Information	9-1
User Codes & Levels of Authority	9-1
Multiple Partition Access	9-2
Adding a Master, Manager, or Operator Code	9-3
Changing a Master, Manager, or Operator Code	9-3
Adding an RF Key to an Existing User	9-4
Deleting a Master, Manager, or Operator Code	9-4
Exiting the User Edit Mode	9-4
SECTION 10: TESTING THE SYSTEM.....	10-1
Battery Test	10-1
Dialler Test	10-1
Burglary Walk-Test (Code + [5] TEST).....	10-1
Armed Burglary System Test	10-2
Testing Wireless Transmitters.....	10-2
Trouble Conditions	10-3
Telephone Operational Problems	10-3
To the Installer	10-4
APPENDIX A: SPECIFICATIONS	A-1
APPENDIX B: CONTACT ID AND EVENT LOG CODES.....	B-1
Table of Contact ID Event Codes	B-1
Table of Event Log Codes	B-2
APPENDIX C: SUMMARY OF SYSTEM COMMANDS	C-1
INDEX.....	INDEX-1
LIMITATIONS & WARRANTY	D-1

List of Figures

Figure 3-1. Installing the Lock	3-1
Figure 3-2. Mounting the PC Board.....	3-1
Figure 3-3. Keypad Connections to Control Panel	3-2
Figure 3-4: Using a Supplementary Power Supply for Keypads.....	3-3
Figure 3-5: Wiring Connections for the Alarm Sounder Output.....	3-3
Figure 3-6: AB12M Bell Box Wiring.....	3-3
Figure 3-7. Standard Telephone Line Connections.....	3-4
Figure 3-8. Australian Phone Connections.....	3-4
Figure 3-9. Zones 1-9 Wiring Connections.....	3-5
Figure 3-10: 2-Wire Smoke Detector Connected to Zone 1	3-5
Figure 3-11. 4-Wire Smoke Detector Power Reset Using 4204 Relay Module.....	3-6
Figure 3-12. Wiring the ASC-SS1T Shock Sensor in Series to Zone 8	3-6
Figure 3-13. Wiring Latching Glassbreak Detectors in Parallel to Zone 8.	3-6
Figure 3-14. Polling Loop Connections	3-7
Figure 3-15. Polling Loop Connections Using One 4297 Extender Module.....	3-8
Figure 3-16. Polling Loop Connections Using Multiple 4297 Extender Modules	3-8
Figure 3-17. 5881EN/5882AP Wireless Receiver	3-9
Figure 3-18a. 5882EUH Wireless Transceiver	3-10
Figure 3-18b. 5882EU Wireless Transceiver	3-10
Figure 3-19. 4204 Relay Module	3-12
Figure 3-20. XM10E Modulator Connection	3-13
Figure 3-21: Wiring the FSA Module	3-13
Figure 3-22. Remote Keypad Sounding Connections	3-14
Figure 3-23. Remote Keyswitch Wiring	3-14
Figure 3-24. Keyswitch by Partition Wiring Connections.....	3-15
Figure 3-25. Auxiliary Alarm Signaling Equipment.....	3-15
Figure 3-26: Panel Linking Block Diagram	3-15
Figure 3-27: VA8200 Panel Link Module Wiring	3-16
Figure 3-28. Event Log Printer Connections	3-17
Figure 3-29: Wiring Long Range Radio to Keypad Terminals.....	3-18
Figure 3-30. 4286 VIP Module Connections	3-20
Figure 3-31. Telephone Line Monitor Connections	3-20
Figure 3-32. AAV Connections to Control Alone	3-22
Figure 3-33. AAV Connections with a 4204	3-22
Figure 3-34. AAV Connections with a 4286	3-23
Figure 3-35. Connections to the Video Transmitter.....	3-24
Figure 3-36: Wiring VistaKey	3-25
Figure 3-37. Wiring the VISTA Gateway Module	3-26
Figure 3-38. AC Mains and Battery Connections	3-26
Figure 3-39. 4300 Transformer Connections	3-26
Figure 3-40. XF10 Transformer Connections.....	3-26
Figure 7-1. Direct Wire Downloading Connections	7-3

Conventions Used in This Manual

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



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



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

ZONE PROG?
1 = YES 0 = NO 0

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

***00**

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

PRODUCT MODEL NUMBERS:

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

General Description

General Description

The VISTA-120IT is an 8-Partition alarm control panel that supports up to 128 zones using basic wired, polling loop, and wireless zones. In addition, the control offers relay control, access control capability, and scheduling capabilities for automating system functions. The major system features are outlined below.

New Features

This version of the VISTA-120IT has enhanced features not found in the prior version.

- Provides a programmable option, which allows the arming of a partition with an AC Loss or Communication Failure present. **Note: The system enters the override of the AC Loss and Comm Fail into the Event Logs as “OVERRIDE TRBUxxx”.**
- Prevents the arming of a partition when a System Low Battery, Telco Fail, or a fault or trouble on zones 800 – 830, 970, 988, 990, or 997 are present. These conditions must either be corrected or bypassed before arming the partition. **Note: Zones 970 (Bell Supervision), 988 and 990 (RF Receiver) and 997 (Polling Loop) cannot be bypassed and therefore, must be corrected before arming the partition.**

Basic Wired Zones

Provides 9 basic wired zones:

- EOLR supervision (optional for zones 1-8) supporting N.O. or N.C. sensors (zone 1 via red jumper on PC board above terminal 10)
- 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
- Up to 50 2-wire latching glassbreak detectors on zone 8

Wireless Expansion

Supports up to 128 wireless zones using 5881EN/5882EU/5882EUH/5882AP type RF Receiver (less if using basic wired and/or polling loop zones).

Wireless zones have the following characteristics:

- Supervised by control panel for check-in signals (except certain non-supervised transmitters)
- Supervised for low battery condition
- Cover removal tamper protection for 5800/5800EU/5800H/5800AP series supervised transmitters
- Wall removal tamper protection for 5800EU/5800H series supervised transmitters
- Individually assignable to one of 8 partitions



For specific information regarding number of wireless zones supported by each RF receiver, see **Wireless Expansion** later in this manual.

Polling Loop Expansion

Supports up to 119 additional wired zones using a built-in polling (multiplex) loop interface. Current drain 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

Peripheral Devices

Supports up to 32 addressable devices, which can be any combination of 6139/6164/5839EU/5839H keypads, RF receivers (5881EN/5882EU/5882EUH/5882AP), relay modules (4204), Fire System Annunciators (FSA-8, FSA-24), panel linking module (VA8200) and the 4286 VIP module or TeleCommand. Peripheral Devices have the following characteristics:

- Terminated at the Keypad Port terminals on the control panel (except for wireless 5839EU/5839H)
- Each device set to an individual address (physically) according to the device's instructions
- Each device enabled in the system using the *Device Programming Mode*

Optional VISTA Interactive Phone Module

Supports the ADEMCO 4286 VIP Module* or TeleCommand**, that permits access via telephone to do the following:

- Obtain system status information
- Arm and disarm security system
- Control relays and/or Powerline Carrier devices
 - * English language version only
 - **English, French, Italian, Spanish, Portuguese and Chinese

Supervisory Zones

Provides zones for supervision of the following:

- Bell Supervision Zone 970
- J7 Trigger Outputs Zone 973
- RF Receivers Zones 988, 990
- Polling Loop Zone 997

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 Acct. No. (or Partition No. if Contact ID reporting is used)

8 Partitions

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

- Up to 3 "Common Area" partitions, which arm automatically when the last partition (1-8) that shares the common area is armed and disarms when the first partition (1-8) that shares the common area is disarmed
- A Master Partition (9) to which keypads may be assigned to view the status of all 8 partitions at the same time
- Keypads assignable to one of 8 partitions or to Master Partition 9 to view system status
- Ability to assign Relays/Powerline Carrier devices to one or all 8 partitions
- 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. Each user, if assigned to more than one partition, retains the same user number across all partitions, and will only utilize one user "slot" in the system. Certain characteristics must be assigned to each user code as follows:

- Authority level for each partition (Master, Manager, or several other Operator levels)
- Opening/Closing central station reporting option
- What partitions the code can operate
- Global arming capability (arm and disarm all partitions the code has access to in one command)
- Use of a wireless transmitter to arm and disarm the system (wireless transmitter must first be "enrolled" into the system)

Pass Point Access Control System (ACS)

If the PassPoint ACS has uncommitted zones, up to 32 of these zones can be used as if they were basic wired zones, as long as they are within VISTA-120IT's total capacity of 128 protection zones.

Keypad Macros

Accommodates up to 4 keypad macro commands per partition (each macro is a series of keypad commands), which can be assigned to the A, B, C and D keys on each partition's keypads.

This means, for example, that by pressing the "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). Each macro can be up to 32 characters in length.

Optional Output Devices (4204 Relays and Powerline Carrier [i.e., X-10] Devices)

Accommodates the use of 32 output devices, which can be a combination of ADEMCO's 4204 Relay Modules or Powerline Carrier Devices (i.e., X-10), and up to 64 polling loop relay outputs (1 per 4101SN). Each 4204 module provides four "Form C" relays for general purpose use.

Powerline Carrier Devices are controlled by signals sent through the electrical wiring at the premises via a 4300 transformer or other appropriate modulator (e.g. XM10E in Europe; XF10 in Australia). Therefore, if using Powerline Carrier Devices, a 4300 (110V) or XF10 (220V) transformer must be used in place of the regular system transformer (plug-pack) in the markets using those devices. Elsewhere, the power transformer and the line carrier modulator are separate (Europe/XM10E).

Output devices have the following characteristics:

- Can activate in response to system events
- Can activate using time intervals
- Can be activated manually using the #70 relay command mode
- Can each have an alpha descriptor assigned to it
- Can be activated remotely from the PC downloader during the download session

Access Control

VISTA-120IT supports the capability with ADEMCO's PassPoint Access Control System (ACS), PassPoint ACS processes card reader information and controls the locking and unlocking of doors. PassPoint also has input zones and output relays/triggers. VISTA-120IT can incorporate uncommitted ACS zones as part of its security system and can control uncommitted ACS relays as if they were part of its own relay group. VISTA-120IT arming stations wired and wireless keypads and RF keys and zones can be used to control doors in the ACS. Conversely, PassPoint access cards can control relays, triggers, and X-10 AC mains signalled devices in the VISTA-120IT system. The arming status of VISTA-120IT partitions can control access through doors in the PassPoint ACS.

If programmed and PassPoint is not used, VISTA-120IT provides users with a command which activates a relay for two seconds to open access doors (e.g. area door). Each partition can be assigned one access control relay. The VISTA-120IT also has built in integrated access control capabilities and can interface with up to 15 VistaKey modules (15 access points), which are used for access control. Each VistaKey is a single-door access control module that supports a proximity reader. The VISTA-120IT can store access control events in the event log.

Up to 250 cardholders can be supported.

Voltage Triggers

Provides a trigger connector whose pins change state for different conditions. Used with Long Range Radio transmitters or other devices such as a voice dialler, a derived channel STU, a remote keypad sounder, keyswitch Armed and Ready LEDs.

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.

In addition, supports **one** keyswitch per partition via use of a serial number multiplex RPM (i.e. 4193SN) with a double pole switch (key removable in both the arm and disarm positions).

Event Log

Keeps a log of different event types (enabled in programming) up to a total of 512 events.

- Can be viewed at the keypad or through the use of Compass upload software
- Can be printed on a serial printer using a 4100SM module as an interface to the control.

Scheduling

- Open/Close schedules (for control of arming/disarming and reporting)
- Holiday schedules (allows different time periods for Open/Close schedules)
- Timed Events (activate relays, auto-bypass/unbypass, auto-arm/disarm, etc.)
- Access schedules (for limiting system access to users by time and/or day)
- End User Output Programming mode (provides 20 timers for relay control)

Audio Alarm Verification Option

Provides a programmable Audio Alarm Verification (AAV) option that can be used in conjunction with an output relay to permit voice dialogue between an operator at the central station and a person at the protected premises.

- Requires the use of an optional AAV unit, such as UVS/UVS-EU
- If used, Zone 5 is no longer available as a protection zone

Video Alarm Verification Option

Provides a programmable Video Alarm Verification (VAV) option, which can be used in conjunction with an output relay to permit video imagery of the protected premises using standard telephone lines.

Requires the use of a Video Transmitter and associated Video Receiver.

Cross-Zoning Capability

Helps prevent false alarms by preventing a zone from going into alarm unless its linked zone is also faulted within five 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) will be bypassed and the system will arm
- Generates an "Exit Error" report by user and by zone so the Central Station knows it was an exit alarm and who caused it

Improved Downloading Speed

Uploads and downloads at 300 baud (predecessor control rate is 75 baud), making upload/download speed approximately four times faster.

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 Expanded High Speed
- ADEMCO Contact ID
- Robofon Contact ID

PSTN (Public Switched Telephone Network) Compatibility

The VISTA-120IT is suitable for use in many national telephone systems around the world, but the specific versions of VISTA-120IT have uniquely designed hardware and software capabilities to meet the PSTN regulation requirements of Norway, Sweden, Finland, Netherlands, Belgium, France and Australia.

Alternative Communications Media Capabilities

- Contact ID messages appear in a special keypad bus data packet that can be extracted by Long Range Radio transmitters, CATV modems and various TCP-IP network interface devices designed to access them.
- Contact ID messages can optionally be transmitted in ASCII through the printer output for RS232C interface to host computers and various network interface devices.
- Supports Dynamic Signaling feature, which prevents redundant signals being sent to the central station when both the built-in dialer and Long Range Radio are used.

Built-in User's Manual and Descriptor

Contains a built-in Users Manual and Descriptor Review mode.

- By pressing and holding any of the keypad function keys for 5 seconds, a brief explanation of that particular function scrolls across the alpha-numeric display.
- By pressing and holding the READY key for 5 seconds and then releasing it, all programmed zone descriptors can be displayed (one at a time). This serves as a check for installers to be sure all descriptors are entered properly.

Partitioning and Panel Linking

Theory of Partitioning

This system provides the ability to arm and disarm up to 8 different areas, each as if it had its own control. These areas are called partitions. Partitions are used when the user desires to disarm certain areas while leaving other areas armed, or to limit access to certain areas to specific individuals. Each user of the system can be assigned to operate any or all partitions, and can be given a different authority level in each.

First, you must determine how many partitions are required (1-8). This must be done before anything can be assigned to those partitions.

Keypads

Each keypad must be given a unique "address" and assigned to one partition (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 can be assigned 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 you want to log on to from another.

Up to 3 partitions can be selected as "common area" partitions, and other partitions can affect these partitions by causing arming/disarming of these partitions to be automated (see *Common Area 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 *SECTION 4: Programming*, as well as each corresponding section's programming procedure.

1. Determine how many partitions the system will consist of (programmed in field 2*00).
2. Assign keypads to partitions (#93 Device Programming mode).
3. Assign zones to partitions (#93 Zone Programming 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 *SECTION 5: Data Field Descriptions*).

Common Area Logic

When an installation consists of one or more partitions shared by users of other partitions in a building, those shared partitions may be assigned as the "common area" partitions for the system (program fields 1*11, 1*14, 1*17). An example of this might be in a medical building where there are two doctor's offices and a common entrance area (see example that follows explanation).

This option employs logic for automatic arming and disarming of the common area. Programming fields affect the way the common area will react relative to the status of other partitions. They are: 1*12, 1*15, 1*18 (Affects Common Area) and 1*13, 1*16, 1*19 (Arms Area).

1*12, 1*15, 1*18 - Affects Common Area (must be programmed by partition)

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

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

1*13, 1*16, 1*19 - Arms Common Area (must be programmed by partition)

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

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



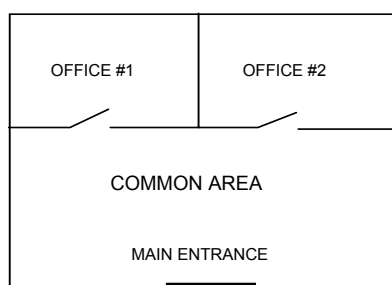
You cannot select a partition to "arm" the common area unless it has first been selected to "affect" the common area. Enable field 1*12, 1*15, 1*18 before enabling field 1*13, 1*16, 1*19 respectively.

The following chart summarizes how the common area partition will operate if different options are set for another partition in fields 1*12, 1*15, 1*18 and 1*13, 1*16, 1*19.

1*12, 1*15, 1*18 Affects Common Area	1*13, 1*16, 1*19 Arms Common Area	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 Common Area would react in a typical setup.



User #1 has access to Office #1 and the Common Area.
User #2 has access to Office #2 and the Common Area.
Office #1 is set up to affect the Common Area, but not arm it.
Office #2 is set up to affect and arm the Common Area.

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

Sequence #1:

	Office 1	Office 2	Common Area 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	Common Area 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 common area also armed (Office #2 is programmed to affect *and* arm the common area). In sequence #2, the common area could not arm when Office #2 armed, because Office #1, which affects the common area, was still disarmed.

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

Common Area Programming Requirements

The following should be considered when assigning common areas.

1. Common areas must be defined in ascending numerical order. That is, the common area containing the lowest partition number should be defined as common area 1 (ex. Do not define partition 8 as common area 1 and partition 1 as common area 2).
2. Common area 1 must be defined before defining common area 2, and common area 2 must be defined before defining common area 3.
3. A common area cannot be designated as an "affecting" and/or "arming" partition of another common area.
4. A partition not defined as a common area can be designated as an "affecting" and/or "arming" partition for more than one common area. If designated as an "arming" partition, it must also be an "affecting" partition

How User Access Codes Affect the Common Area

Codes with "Global" Arming

If a code is given "global arming" when it is defined (see *SECTION 10: Security Access Codes*), the keypad will ask "Arm all?" or "Disarm all?" whenever the user tries to arm or disarm the partitions he has access to from a keypad. This allows the user to pick and choose the partitions to be armed or disarmed, and so eliminates the "automatic" operation of the common area. 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 common area, and the message "UNABLE TO ARM COMMON AREA PART" will be displayed.

Codes with "Non-Global" Arming

If arming with a non-global code, the common area partition operation will be automatic, as described by fields 1*12, 1*15, 1*18 and 1*13, 1*16, 1*19.

Other Methods of Arming/Disarming

When arming or disarming a partition that affects and/or arms the common area in one of the following manners, common area logic remains active:

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

Arming/Disarming Remotely

If arming or disarming remotely (through Compass downloading software), the common area will not automatically follow another partition that is programmed to arm or disarm the common area. The common area 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 area partition will not automatically follow another partition that is programmed to arm or disarm the common area. The common area must be included as a partition to be armed/disarmed.



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 common area. This will cause the common area 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 #93 Device Programming mode will become 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 security officer in a building to have to "log-on" to various partitions from one partition's keypad to find out where an alarm has occurred.

The following is an example of a typical display:

SYSTEM	1	2	3	4	5	6	7	8
STATUS	R	R	N	N	A	T	B	A

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). 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 onto Partition 9 to view the status of *all* partitions, that user must have access to all partitions. Otherwise, access will be denied.

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

WHSE DISARMED KEY * FOR FAULTS

This is the normal display that appears at Partition 1's keypad(s). Pressing [*] will display:

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.]. This will display the status of the new partition.

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 that are disarmed are "ready to arm." Neither LED will be lit if only some partitions are armed and only some disarmed 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)

The sounder may be silenced by pressing any key on the Master keypad or a keypad in 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 in Partition 1. Therefore, panics must be programmed for Partition 1.

Panel Linking

Up to eight VISTA-120IT control panels may be locally networked, enabling a user to control the features of all control panels from a single location. The panel linking bus supports an end-to-end network length of up to 1220m, making it ideal for multi-building environments (e.g., a shopping mall, college campus, etc.).

Panel linking requires a VA8200 Panel Link Module (PLM) on each VISTA-120IT. Users can link (access other control panels) in any of three different modes: Single-Partition, Single-Panel Mode; Multi-Partition, Multi-Panel Mode; Multi-Panel View Mode. These modes are described later in this section.

Each PLM connects to the ECP bus on the control panel and communicates to each PLM via an RS-485 bus (3-wire twisted cable run) with a maximum wire-run of 1220m end-to-end.



Users 001-050 are the only users that can perform panel linking and are automatically assigned panel linking access when added to the system.
An alpha keypad must be used for panel linking.
The system may take up to 7 seconds to respond to a command when in a panel linking mode

NOTE: A user cannot access partitions or panels to which they have not been assigned.

Panel Link Module Supervision

The Panel Link Module can be supervised for its connection to the control panel. The module's supervisory zone is zone 8xx, where "xx" = the ECP address of the PLM. You must program that zone with response type 05 (Day/Night) in *Zone Programming* in the #93 Menu Mode (refer to the *Programming Guide* for detailed programming instructions). If you want to report the supervisory failure to the central station and/or to a paging service, the appropriate reporting parameters for that zone must be programmed.

If you want the supervisory failure of PLM(s) on other linked control panels to display on this control panel, they must be programmed into *Zone Programming* in the #93 Menu Mode with response type 14 in this control panel (refer to the *Programming Guide* for detailed programming instructions). The panel ID number for each module must match the panel ID number programmed in *Device Programming* of its "host" VISTA-120IT.

How to Use Panel Linking

Panel Linking can be used in any of three different modes:

- Single-Partition, Single-Panel – displays status of a partition on a remote control panel and allows control of that remote control panel.
- Multi-Partition, Multi-Panel Mode – displays status and allows arming/disarming of multiple partitions at once on a remote control panel.
- Multi-Panel View Mode – displays status and allows arming/disarming of multiple remote control panels at a time.

NOTE: A user will not be able to access or view partitions or panels to which they have not been assigned.

Single-Partition Single-Panel Mode

To access the Single-Partition, Single Panel mode, perform the following steps:

Step	Action
1	Enter User Code (for users 001-050) + [#] + [86] .
2	Enter the panel ID number (01-08) of the panel to which you want to link.
3	Enter the partition number of the panel. The keypad displays "AWAITING PANEL LINK." After a few seconds, the keypad displays the status of the partition along with the panel ID number and partition number flashing in the upper right-hand corner. The user now has full control of the remote control panel. All functions can be performed except the following: <ul style="list-style-type: none"> • Those limited by the user's authority level. • The user cannot enter Installer Program mode. • The user cannot execute another panel linking mode. NOTE: To execute another panel linking mode or to access a different remote panel, the user must first exit this mode (return to the original control panel).
4	To exit, enter the User Code (for users 001-050) + [#] + [85] . After a few seconds, the keypad displays the status of the original partition for the keypad.

Multi-Partition Multi-Panel Mode

To perform a function in the Multi-Partition, Multi Panel mode, follow the steps below:

Step	Action																																	
1	<p>Enter User Code (for users 001-050) + [#] + [88].</p> <p>The keypad displays the following:</p> <table><tr><td>PANELnn</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr><tr><td>STATUS</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td></tr></table> <p>where “nn” = panel ID number (01-08), “12345678” are the partition numbers and “xxxxxxx” is the status of each partition of that panel. Status indications include:</p> <table><tr><td>A = Armed Away</td><td>S = Armed Stay</td><td>M = Armed Maximum</td></tr><tr><td>I = Armed Instant</td><td>R = Ready</td><td>N = Not Ready</td></tr><tr><td>B = Bypassed/Ready</td><td>* = Alarm</td><td>T = Trouble</td></tr><tr><td>F = Fire Alarm</td><td>P = AC Power Failure</td><td>L = Low System Battery</td></tr><tr><td>C = Comm Fail</td><td></td><td></td></tr></table> <p>NOTES: See table later in this section for priority of displays.</p> <p>A “•” under a partition number indicates the user does NOT have access to that partition.</p>	PANELnn	1	2	3	4	5	6	7	8	STATUS	x	x	x	x	x	x	x	x	A = Armed Away	S = Armed Stay	M = Armed Maximum	I = Armed Instant	R = Ready	N = Not Ready	B = Bypassed/Ready	* = Alarm	T = Trouble	F = Fire Alarm	P = AC Power Failure	L = Low System Battery	C = Comm Fail		
PANELnn	1	2	3	4	5	6	7	8																										
STATUS	x	x	x	x	x	x	x	x																										
A = Armed Away	S = Armed Stay	M = Armed Maximum																																
I = Armed Instant	R = Ready	N = Not Ready																																
B = Bypassed/Ready	* = Alarm	T = Trouble																																
F = Fire Alarm	P = AC Power Failure	L = Low System Battery																																
C = Comm Fail																																		
2	<p>The following functions can be performed:</p> <p>Press [1] to attempt to disarm all partitions.</p> <p>Press [2] to attempt to arm AWAY all partitions.</p> <p>Press [3] to attempt to arm STAY all partitions.</p> <p>Press [4] to attempt to arm MAXIMUM all partitions.</p> <p>Press [7] to attempt to arm INSTANT all partitions.</p> <p>Press [*] to read the status of the next panel.</p> <p>Press [#] key to read the status of the previous panel.</p> <p>Press [0] to exit mode. After a few seconds, the keypad displays the status of the original partition of the original panel for the keypad. Also, this mode will end in approximately 120 seconds if no keys are pressed.</p> <p>NOTES: When performing any of the arming commands, if there are faults in any of the partitions, none of the partitions will arm. These faults must be corrected or bypassed before attempting to arm.</p> <p>The user cannot execute another panel linking mode. To execute another panel linking mode or to access a different remote panel, the user must first exit this mode (return to the original control panel).</p>																																	

Multi-Panel View Mode

To perform a function in the Multi-Panel View mode, follow the steps below:

Step	Action															
1	<p>Enter User Code (for users 001-050) + [#] + [87].</p> <p>The keypad provides the following typical display:</p> <div><div>ALLPANEL 1 2 3 4 5 6 7 8 STATUS x x x x x x x x</div></div> <p>where “12345678” are the panel ID numbers and “xxxxxxx” is the priority status of each panel. Status indications include:</p> <table><tr><td>A = Armed Away</td><td>S = Armed Stay</td><td>M = Armed Maximum</td></tr><tr><td>I = Armed Instant</td><td>R = Ready</td><td>N = Not Ready</td></tr><tr><td>B = Bypassed/Ready</td><td>* = Alarm</td><td>T = Trouble</td></tr><tr><td>F = Fire Alarm</td><td>P = AC Power Failure</td><td>L = Low System Battery</td></tr><tr><td>C = Comm Fail</td><td></td><td></td></tr></table> <p>NOTE: See table later in this section for the priority of displays.</p>	A = Armed Away	S = Armed Stay	M = Armed Maximum	I = Armed Instant	R = Ready	N = Not Ready	B = Bypassed/Ready	* = Alarm	T = Trouble	F = Fire Alarm	P = AC Power Failure	L = Low System Battery	C = Comm Fail		
A = Armed Away	S = Armed Stay	M = Armed Maximum														
I = Armed Instant	R = Ready	N = Not Ready														
B = Bypassed/Ready	* = Alarm	T = Trouble														
F = Fire Alarm	P = AC Power Failure	L = Low System Battery														
C = Comm Fail																
2	<p>The following functions can be performed::</p> <p>Press [1] to attempt to disarm all partitions on all panels.</p> <p>Press [2] to attempt to arm AWAY all partitions on all panels.</p> <p>Press [3] to attempt to arm STAY all partitions on all panels.</p> <p>Press [4] to attempt to arm MAXIMUM all partitions.</p> <p>Press [7] to attempt to arm INSTANT all partitions.</p> <p>Press [0] to exit mode. After a few seconds, the keypad displays the status of the original partition of the original panel for the keypad. Also, this mode will end in approximately 120 seconds if no keys are pressed.</p> <p>NOTES:</p> <p>When performing any of the arming commands, if there are faults in any of the partitions of a panel, the system will not arm that panel, but will arm all the other partitions of the other panels.</p> <p>The user cannot execute another panel linking mode. In order to perform another panel linking mode or to access a different remote panel, the user must first exit this mode (return to the original control panel).</p>															

Priority of Displays for Multi-Partition and Multi-Panel Modes

This table shows the priority of displays if more than one of these conditions exists at the same time.

Priority	Description	Display	Priority	Description	Display
1	Fire Alarm	F	8	Not Ready	N
2	All Other Alarms	*	9	Ready	R
3	AC Loss	P	10	Armed STAY	S
4	Comm Fail	C	11	Armed AWAY	A
5	System Low Battery	L	12	Armed INSTANT	I
6	Trouble	T	13	Armed MAXIMUM	M
7	Bypass	B			

For example, if you are in the Multi-Partition Mode and a partition has a zone with a trouble condition, a zone bypassed, and a zone faulted, the system displays “T” for the Trouble.

If you are in Multi-Panel Mode and one of the panels has one partition armed STAY, a second partition armed AWAY and a third partition armed INSTANT, the system displays “S” for STAY.

Installing the Control

Mounting the Cabinet

1. 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.
2. 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

1. Remove cabinet door, then remove the lock knockout from the door. Insert the key into the lock.
2. Position the lock in the hole, making certain that the latch will make contact with the latch bracket when the door is closed.
3. When correctly positioned, push the lock until it is held securely by its snap tabs.
Use an ADEMCO No. K4445 Lock (supplied).

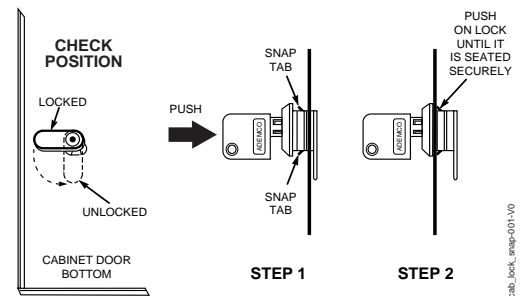


Figure 3-1. Installing the Lock

Installing the Control's Circuit Board

Refer to the Mounting the PC Board *Figure 3-2*.

1. Hang the three mounting clips on the raised cabinet tabs. Make sure the clip orientation is exactly as shown in *Figure 3-2* 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 in step 2 detail.
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 insures 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 minimizing the risk of panel RF interference with television reception.

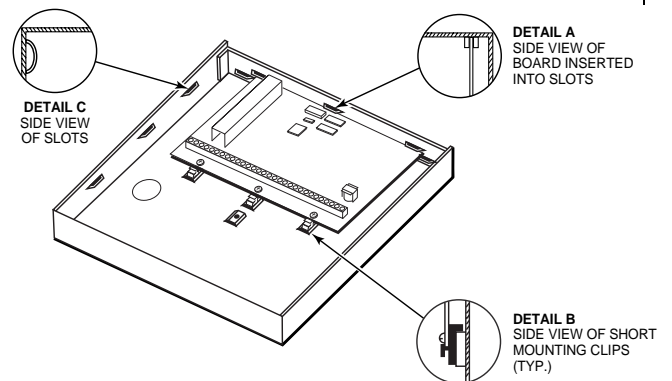


Figure 3-2. Mounting the PC Board

Installing the Keypads

- Two Line Alpha Display wired 6139/6164 and wireless 5839EU/5839H
- Up to 32 addressable devices, including keypads, may be used in the system, as long as the auxiliary current is available (you may need to use an auxiliary power supply if the 750mA auxiliary output is exceeded)

To install the keypads, perform the following steps:

- Mount the keypads at a height that is convenient for the user. Refer to the instructions provided with the keypad for mounting procedure. Refer to the mounting instructions and template included with the keypad for specific information.
- Determine wire size by referring to the wiring length/size chart below.
- 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 single keypad, which is wired back to the control, must not exceed the lengths listed in the table.

Wire Run Length/Size Table	
Wire Size	Length
0.64 mm	137 m
0.81 mm	213 m
1.0 mm	335 m
1.3 mm	533 m



The length of all wire runs combined must not exceed 610 metres when unshielded quad conductor cable is used (305 metres if shielded cable 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 (i.e. the maximum length would be 69 metres if two keypads are wired using 0.64mm diameter wire).

For keypads connected to a single 4-wire run, determine the current used by all units connected to the single wire run, then refer to the Wiring Run chart to determine the maximum wire length that can be safely used for each wire size. Current drain for each device can be found in the Installation Instructions accompanying the device.

- Run field wiring from the control to the keypads (using standard 4-conductor twisted wire cable using the wire size determined in step 1).
- Connect keypads to the Keypad Port terminals 6, 7, 8, and 9 on the control board, as shown below.

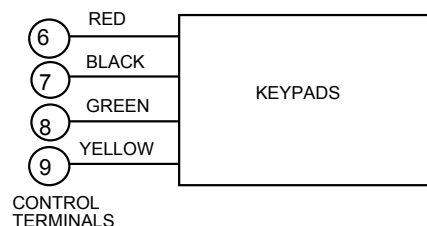


Figure 3-3. Keypad Connections to Control Panel

Addressing the Keypads



The keypads will not operate until they are assigned an address and enabled in the system's Device Programming Mode.

Set each keypad to an individual address (00-30) according to the keypad's instructions. Set one alpha keypad for address "00" and other keypads for higher addresses (01, 02, and 03 are enabled in the system's default program). Any keypads set for address 04 and above will appear blank until they are enabled in the system's program.



Keypads set to the non-addressable mode (address 31) may interfere with other keypads (as well as other devices) connected to the keypad terminals.

Using a Supplementary Power Supply to Power Additional Keypads

The control provides 750mA of auxiliary standby power for powering keypads and other devices from the auxiliary power output. Aside from this, the control can support up to 32 peripheral devices (keypads, RF receivers, relay modules, etc.). The backup battery will supply power to these devices in the event that AC power is lost. 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., AD12612). The AD12612 power supplies have a backup battery that can power these keypads in the event of AC mains power loss.



Keypads powered from supplies which do not have a backup battery **will not function** when AC mains is lost. Therefore, be sure to power at least one keypad from the Control's auxiliary power output.

Connect additional keypads as shown below using the keypad wire colours shown. Be sure to observe the current ratings for the power supply used.



Make connections directly to the screw terminals as shown. Make no connection to the keypad blue wire (if present). Be sure to connect the negative (–) terminal on the Power Supply unit to terminal 7 (AUX –) on the control.

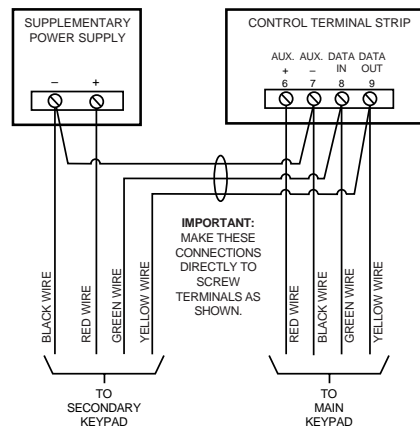


Figure 3-4: Using a Supplementary Power Supply for Keypads

Installing External Sounders

The Control provides one bell/siren relay output used to power external alarm sounders. This output is rated at 10-13.8VDC, 2.8A maximum (including auxiliary current drain).



Exceeding the prescribed current limits will overload the power supply or may possibly trip the bell output circuit protector.

The total current drain from this output can be up to 2.8 amps. A battery must be installed since current in excess of 750mA is supplied by the battery. Up to two 702 sirens can be used, wired in series. Up to two 719 sirens can be used wired in parallel.

Compatible Sounders

Model Number	Device Type	Description
702	Outdoor Siren	Self-contained siren (driver built-in) and weatherproof for outdoor use. Can be wired for either a steady or yelp sound and is rated at 120 dB @ 3m. This siren can also be tamper protected, or can be mounted in a metal cabinet (716), which can be tamper protected.
719	Compact Outdoor Siren	Compact, self-contained siren (driver built-in), and weather proof for outdoor use. Can be wired for either a steady or yelp sound, and is rated at 90 dB @ 3m. A 708BE cabinet is available, which can be tamper protected if necessary.
747 747F WAVE2	Indoor Siren	Attractive, self-contained indoor siren (driver built-in), provides steady or warble tones and is rated at 95dB @ 3m.
WAVE2EX	Indoor Piezo Sounder	System Sensor indoor piezo sounder, rated at 90 dB @ 3m.
AB12M	Armoured Bell	For High Security Commercial Burglary installations.

Wiring the Alarm Output

Make the wiring connections to terminals 4 (positive output) and 5 (negative return).

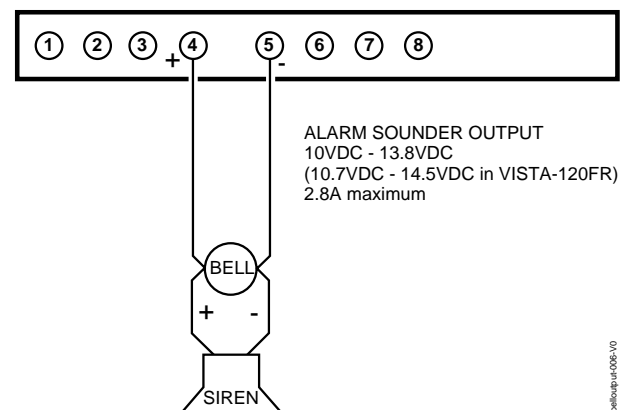


Figure 3-5: Wiring Connections for the Alarm Sounder Output

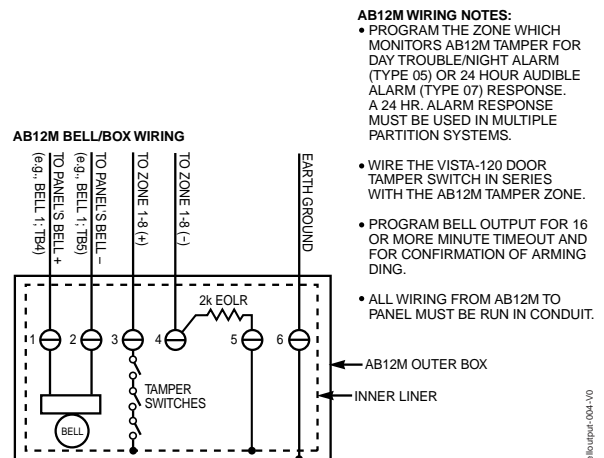


Figure 3-6: AB12M Bell Box Wiring

AB12M WIRING NOTES:

- PROGRAM THE ZONE WHICH MONITORS AB12M TAMPER FOR DAY TROUBLE/NIGHT ALARM (TYPE 05) OR 24 HOUR AUDIBLE ALARM (TYPE 07) RESPONSE. A 24 HR. ALARM RESPONSE MUST BE USED IN MULTIPLE PARTITION SYSTEMS.
- WIRE THE VISTA-120 DOOR TAMPER SWITCH IN SERIES WITH THE AB12M TAMPER ZONE.
- PROGRAM BELL OUTPUT FOR 16 OR MORE MINUTE TIMEOUT AND FOR CONFIRMATION OF ARMING DING.
- ALL WIRING FROM AB12M TO PANEL MUST BE RUN IN CONDUIT.

bellbox-wiring-004-v0

bellbox-wiring-005-v0

Programming Option

Program field *08 permits the external sounder output to be altered so that it is activated normally to charge the battery in a self-actuated external sounder and is interrupted for alarm conditions (continuously for intrusion/audible panic sounding and pulsed for fire alarm sounding).

Standard Phone Line Connections

1. Connect the incoming phone line and handset wiring to the main terminal block as follows (see Standard Telephone Line Connections *Figure 3-7*), (Does not pertain to Australia)
 TB1-26: Local Handset (TIP)
 TB1-27: Local Handset (RING)
 TB1-28: Incoming Phone Line (TIP)
 TB1-29: Incoming Phone Line (RING)
2. In Australia, plug the phone cord into the jack on the control's PCB.



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



To supervise for a fault on the telephone line, install the ADEMCO 659EN Telephone Line Monitor. Connect the output to zone 009 and program the zone with Response Type 05 (Day/Night).

PABX

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. Many PABXs are not power backed up and connection to such a PABX will result in a communication failure if power is lost.

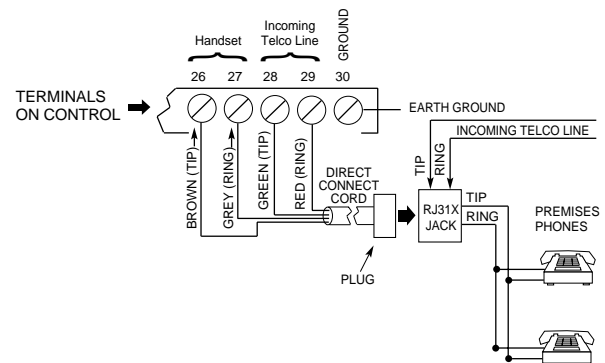


Figure 3-7. Standard Telephone Line Connections

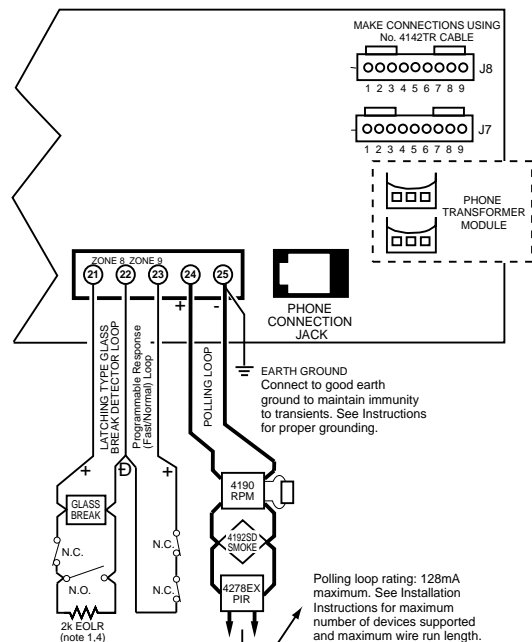


Figure 3-8. Australian Phone Connections

Wiring Devices to Zones 1-9

Connect sensors/contacts to the basic wired zone terminals (10 through 23).

1. Connect N.C. devices **in series** with the high (+) side of the loop. The 2K EOL resistor must be connected in series with the devices, following the last device on zones 1-8.
2. Connect N.O. devices **in parallel (across)** the loop. Observe polarity when wiring smoke detectors. The 2K EOL resistor must be connected across the loop wires at the last device on zones 1-8.

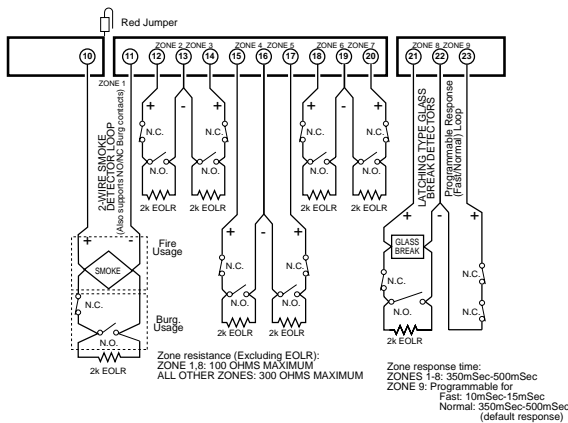


Figure 3-9. Zones 1-9 Wiring Connections



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

Wiring 2-Wire Smoke Detectors to Zone 1

Zone 1 has the added capability of supporting 2-wire smoke detectors. This zone provides enough standby current (2 mA) to power up to sixteen of the smoke detectors listed on the following page. Each zone provides only enough alarm current (20 mA) to power one smoke detector in the alarmed state. When assigned zone type 9, the second entry of a Security Code + OFF sequence at a keypad will interrupt power to this zone to allow detectors to be reset following an alarm.

1. Connect 2-wire smoke detectors across zone 1 terminals (10 & 11) as shown below. Observe proper polarity when connecting the detectors.
2. If an EOL resistor is presently connected across zone 1 terminals, remove it. **The EOL resistors 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.

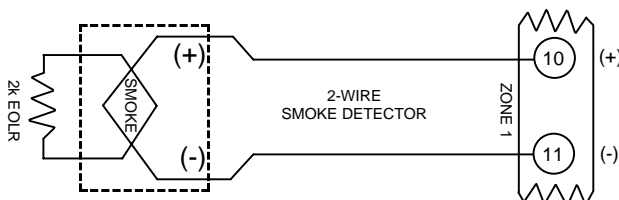


Figure 3-10: 2-Wire Smoke Detector Connected to Zone 1

Compatible 2-Wire Smoke Detectors

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

DETECTOR TYPE	DEVICE MODEL #
Photoelectric, plug-in head	System Sensor 2600EC
Photoelectric, direct wire	System Sensor 2400
Photoelectric w/heat sensor, direct wire	System Sensor 2400TH
Photoelectric w/B401B base	System Sensor 2451
Photoelectric w/heat sensor and B401B base	System Sensor 2451TH
Ionisation, plug-in head	System Sensor 1600EC
Ionisation, direct wire	System Sensor 1400
Photoelectric duct detect. w/DH400 base	System Sensor 2451
Ionisation, plug-in head	System Sensor 1451
Ionisation w/B110LP base	System Sensor 1151
Photoelectric, direct wire	System Sensor 2100
Photoelectric w/heat sensor, direct wire	System Sensor 2100T
Photoelectric w/B110LP base	System Sensor 2151

Unsupervised Usage of Zone 1

Zone 1 can also be used for normally closed, unsupervised devices by doing the following:

1. Cut the red jumper on the PC board located above Zone 1.
2. Connect closed circuit devices in series with terminals 10 and 11.

Wiring 4-Wire Smoke Detectors to Zones 1-8

When programmed for fire warning usage, all zones can monitor 4-wire smoke detectors or N.O. fire alarm initiating 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.



Auxiliary power to 4-wire smoke detectors is not automatically reset after an alarm and therefore must be momentarily interrupted using either a normally-closed momentary switch wired in series with one side of the aux. power to the smokes, or using a 4204 relay as described below.

Using a 4204 relay allows the detectors to be reset via the second entry of a Security Code + OFF sequence. The 4204 relay must be programmed to activate on Zone Type/System Operation 54 (Fire Zone Reset). Refer to #93 Menu Mode Programming in the Programming Guide for more information.

1. Connect 12 volt power for the detectors from Auxiliary Power terminals 6 and 7 as follows:
 - Wire the [+] side of Auxiliary Power (Terminal 6) to the N.C. contact of the 4204 relay.
 - Wire the Center Arm or Pole of the Relay to the [+] Power side of the smoke detector.
2. Connect the [-] side of the smoke detector to [-] Aux. Power (Terminal 7). Observe proper polarity when connecting detectors (see Figure 3-11).

NOTE: Power to 4-wire smoke detectors should be supervised (use a System Sensor A77-716-01 EOL relay module connected as shown).

- Connect detectors (including heat detectors, if used) across terminals of the zone selected. All detectors must be wired in parallel. Remove the 2000 ohm EOL resistor if connected across the selected zone terminals. **You must connect the EOL resistor across the loop wires at the last detector.**

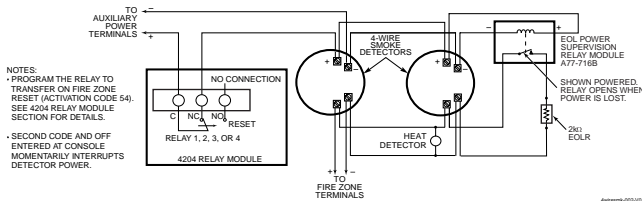


Figure 3-11. 4-Wire Smoke Detector Power Reset Using 4204 Relay Module

Compatible 4-Wire Smoke Detectors

Use any 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 2412B
Photoelectric w/heat sensor, direct wire	System Sensor 2412THB
Ionisation, direct wire	System Sensor 1412B

Wiring 2-Wire Latching Glassbreak Detector To Zone 8

Use zone 8 for connection of compatible 2-wire latching-type glassbreak detectors. Connect all detectors in parallel across zone 8 (terminals 21 and 22).

Remove the 2000 ohm EOL resistor if connected across the selected zone terminals. You must connect the EOL resistor across the loop wires at the last detector.

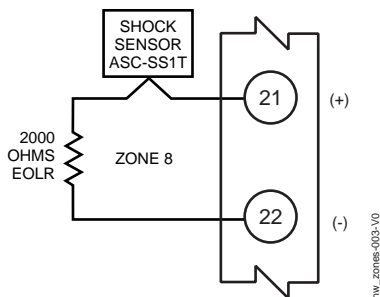


Figure 3-12. Wiring the ASC-SS1T Shock Sensor in Series to Zone 8

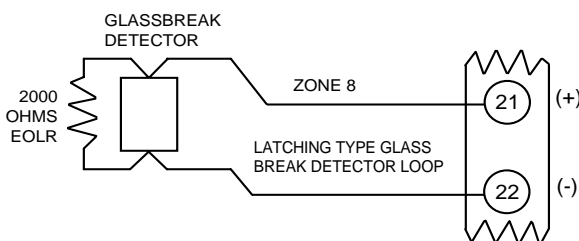


Figure 3-13. Wiring Latching Glassbreak Detectors in Parallel to Zone 8.

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:	2 mA–10 mA
Reset Time:	Less than 6 seconds

NOTES:

The IEI 735L series detectors and ASC-SS1T shock sensors have been tested and found to be compatible with these ratings. You can use up to fifty IEI 735L detectors connected in parallel. You can use up to four ASC-SS1T sensors connected in series.

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



The alarm current provided by zone 8 will support only one Glass Break detector in the alarmed state.



Do not use other NO or NC contacts when using glassbreak detectors on zone 8. Other contacts may prevent proper glassbreak detector operation. If latching type devices are installed on both zones 1 and 8, both zones should be assigned to the same partition. If they are not, and both devices are in alarm at the same time, the resetting of one could cause a loss of alarm memory in the other.

Zone 9 Applications

This zone is unsupervised and is suitable for monitoring fast-acting glass break sensors or vibration sensors. When using zone 9, keep the following in mind:

- Use only closed circuit devices connected in series with one another.
- Program zone 9 as any response type **except** fire (type 09) or panic (types 6, 7 or 8)
- Program fast (10 msec) or normal (350 msec-500 msec) response in data field *14.



Avoid using mechanical magnetic or relay type contacts on zone 9 when programmed for fast response.

Installing Polling Loop Devices

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 connected to the polling loop communicates 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, and is constantly monitoring the status of all zones enabled on the loop.

The maximum current drain of all devices on the polling loop cannot total more than 128mA (unless using a 4297 Polling Loop Extender Module).



Although each polling loop device is wired in parallel, each device has its own unique zone number (or group of zones). On some devices, this is determined by the setting of DIP switches. Other devices have a built-in unique serial number that must be "enrolled" into the control. Serial number mode **MUST** be used instead of DIP switch addressing mode for devices that can be set for either mode.

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



The Quest 2260SN can be programmed as a "Smart Contact" in *Zone Programming*. This prevents those sensors from displaying faults during the disarmed state. You cannot mix "Smart Contacts" with non-"Smart Contacts" in the system.

Compatible Polling Loop Devices

Model No.	Type
998MX	Serialized Dual PIR
4101SN	Serialized Single-Output Relay Module
4190SN	Serialized 2-Zone Expander
4190WH	2-Zone Expander
4191SN	Serial Number Recessed Reed Contact
4193SN	Serialized 2-Zone Expander
4208U	Universal 8-Zone Expander
4275EX	Dual PIR
4275EX-SN	Serialized Dual PIR
4278EX	Quad PIR
4278EX-SN	Serialized Quad PIR
4293SN	Serialized 1-Zone Expander
4297	Extender Module
4939SN-BR	Serial Number Surface-Mount Reed Contacts
4939SN-GY	
4959SN	Serialized Aluminum Overhead Door Contact
5192SD	Serialized Photoelectric Smoke Detector
5192SDT	Serialized Photoelectric Smoke Detector w/Heat Sensor
9500SN	Serialized Dual Technology Glassbreak Detector
QUEST 2260SN	Serialized Dual Technology Smart Motion Sensor

To install the devices perform the following steps:

- Run wires to each device on the polling loop using the the following table for maximum wire runs per wire size. Twisted pair wire is recommended for all wire runs. Maximum total wire runs combined must not exceed 1220m regardless of wire size (610m if shielded wire is used).

Maximum Polling Loop Wire Runs

Wire Size	Max. Length
0.64 mm O.D.	198 m
0.81 mm O.D.	290 m
1.0 mm O.D.	457 m
1.3 mm O.D.	732 m



For new polling loop installations, always use twisted pair wiring. In many cases, existing non-twisted pair wiring may be used, but it is more susceptible to interference from other sources, and may be problematic in installations with long wire runs or in high noise environments.

Always locate polling loop wiring at least 15cm of AC power, telephone, or intercom wiring.

The polling loop carries data between the control panel and the devices; interference on this loop can cause an interruption of communication. The polling loop can also cause outgoing interference on the intercom or phone lines. If this spacing cannot be achieved, shielded wire must be used. (Note that the maximum total wire length supported is cut in half when shielded wire is used.)

- Wire each device to the polling loop, making sure to use correct polarity when making connections (refer to the device's instructions).
- Note the polling loop devices that have DIP switches on them. 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 found at the end of this manual when setting addresses.

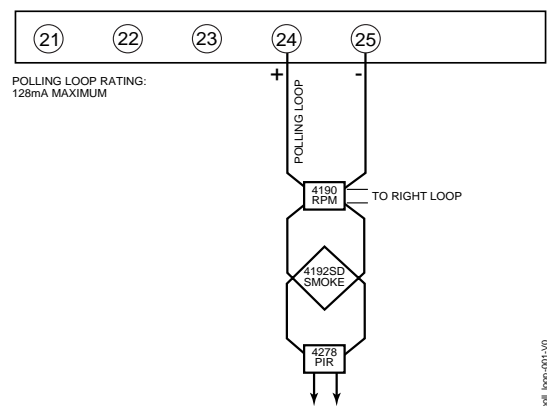


Figure 3-14. Polling Loop Connections

Polling Loop Limitations



Twisted-pair is recommended for all wire runs. 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 1220m (610m if you are using unshielded wire in conduit or shielded wire).

IMPORTANT NOTE: If the installation exceeds or deviates from these parameters, refer to the application note on the Honeywell website for additional information. To access the application note:

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

The built-in polling loop has the following limitations that must be observed:

- The maximum allowable current drain from the polling loop is 128mA. If device drain totals more than 128mA, a 4297 Polling Loop Extender Module is required.
- The 4297 Polling Loop Extender Module may be used to provide additional polling loop current, to extend the polling loop wire run, and/or to provide individual, electrically isolated polling loops. Refer to the 4297 Polling Loop Connection *Figures 3-15 and 3-16* later in this section.



Use of more than 50 DIP switch devices can greatly impact the panel's ability to respond to a change in status in a timely manner. DIP switch devices that affect response time include 4278EX, 4275EX, and 4190WH.



DO NOT use the 4197 Polling Loop Extender Module with the VISTA-120IT.

- Regardless of current drain, no more than 64 DIP switch devices or 119 serial number devices can be connected to the polling loop. Installations that require up to 119 zones using DIP switch devices will require the use of zone expanders (4190WH and/or 4208U), which allow more than one zone on each expander. Otherwise, a 4297 Polling Loop Extender must be used.



Make certain to include the total current drain on the polling loop when figuring the total auxiliary load on the panel's power supply (see *Calculating the Battery Size Needed* later in this section).

Notes: - Do not use the 4197 module with VISTA-120.
- Refer to 4297 instructions for more detailed installation information.

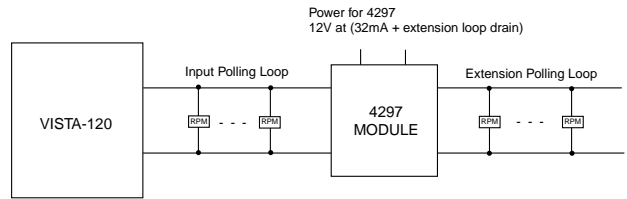


Figure 3-15. Polling Loop Connections Using One 4297 Extender Module

Notes: - Do not use 4197 module with VISTA-120.
- 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.

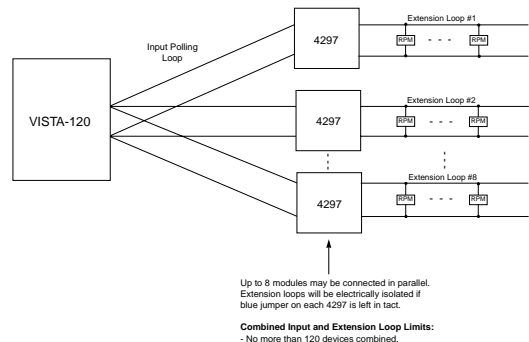


Figure 3-16. Polling Loop Connections Using Multiple 4297 Extender Modules

Polling Loop Supervision

An overload on the polling loop is indicated by a trouble on its supervisory zone (997) and reports as a trouble condition only, even if the system is armed. As such, it should be assigned zone type 05 if annunciation 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, the zones associated with that device will cause an alarm on the corresponding partition(s).



A trouble on Zone 997 will prevent a partition from being armed, even if all polling loop zones on that partition are bypassed. The trouble must be corrected before the partition can be armed.

Maintenance Signal Support

The control monitors maintenance signals from certain smoke detectors (5192SD, 5192SDT). Maintenance signals are triggered when a detector gets dirty. The detector should be cleaned or replaced. If a detector maintains a high or low sensitivity condition for longer than 24 hours, the control sends a dialler report (trouble message for non-Contact ID reports; event code 385 or 386 for Contact ID reports), makes an event log entry, and displays HSENSxxx or LSENSxxx at the keypads (xxx = zone number).

Wireless (RF) Zone Expansion

The VISTA-120IT supports wireless zones that may be used exclusively or in addition to basic wired and/or polling loop zones. The system supports the 5800 series RF system using the following receivers:

5800 Series		5800EU Series	
Rcvr	Zones	Rcvr	Zones
5881ENL	up to 8	5882EU	up to 128
5881ENM	up to 16	5882AP	up to 128
5881ENH	up to 128	5882EUH	up to 128

Wireless System Operation and Supervision

- The receiver responds to status and alarm signals from wireless transmitters [345 MHz (5800 series), 315MHz (5800AP series), 433.92MHz (5800EU series), and 868.095 MHz (5800H series)] within a nominal range of 60m, and relays this information to the control.
- Each 315/345MHz supervised transmitter sends a supervisory signal to the receiver every 70-90 minutes (433.92MHz transmitters transmit every 23-26 minutes and 868.095 MHz transmitters transmit every 9 minutes).
If, after a programmed interval of time (e.g., 24 or 2 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.
The trouble will not prevent you from arming the panel, as long as the zone is first bypassed.
- If, within a programmed interval of time (e.g., 24 or 2 hrs), the receiver does not hear from *any* of its transmitters, a CHECK or TRBL message appears for zones 988 (2nd receiver) or 990 (1st receiver) if zone type 05 is assigned to these supervisory zones. This may be an indication that the wireless receiver is not able to "hear" signals. The same indications are provided if the 5882EU/5882EUH transceiver detects that it is being jammed by a source of RF energy that is present for 30 seconds within any 60-second interval.
- 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 receiver zone number (8xx, where xx = receiver's device address) if type 05 is assigned to these supervisory zones. This 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 panel's Device Programming mode.
- Two identical receivers can be used to provide either a greater area of coverage, or to provide redundant protection.
- Any zone from 1-128 can be used as a wireless zone, with the exception of zone 64 (reserved for a wireless keypad).

Wireless System Installation Advisories

- Place the receiver in a high, centrally located area for best reception. Do not place receiver on or near metal objects. This will decrease the range and/or block transmissions. Do not mount receivers or transmitters in an attic, where extreme temperatures could prevent proper operation.
- For maximum range, install the wireless receiver at least 3 metres 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 3m from each other, as well as from the Control panel and remote keypads.
 - Each receiver must be set to a different Device Address (01-07). The receiver set to the lower address is considered the 1st wireless receiver for supervisory purposes.
 - The house IDs must be the same if using a 5827/5827AP/5827BD wireless keypad.
 - Using two Receivers *does not* increase the number of transmitters the system can support.

Installation and Setup of the 5881EN/5882EU/5882AP Wireless Receivers

- Mount the receiver(s). Receivers must be mounted externally to the control and can detect signals from transmitters within a nominal range of 60m. Take this into consideration when determining mounting location.
- Connect the receiver's wire harness to the control's keypad terminals (6, 7, 8, and 9). Plug the connector at the other end of the harness into the receiver.
- Refer to the installation instructions provided with the receiver for further installation procedures regarding antenna mounting, etc.
- 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.).

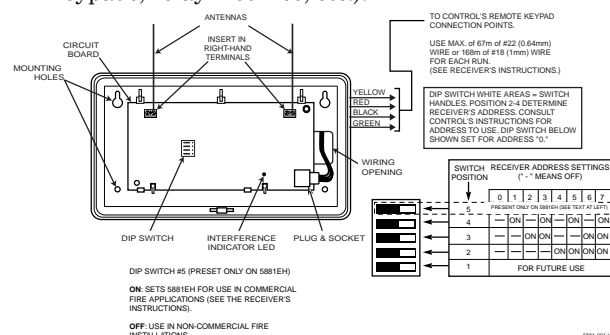
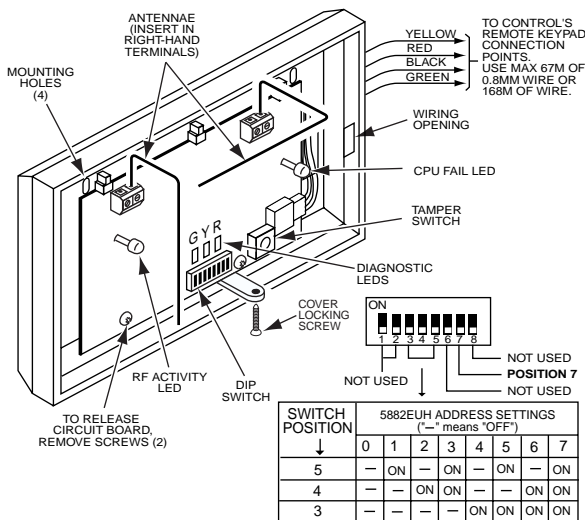


Figure 3-17. 5881EN/5882AP Wireless Receiver

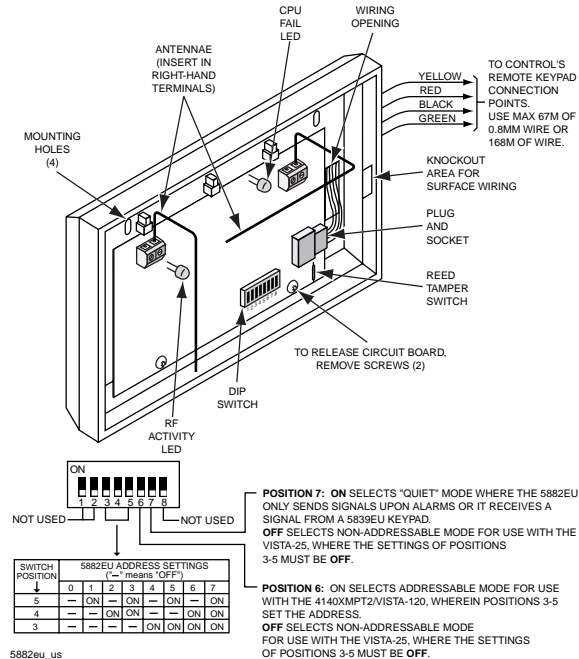


POSITION 7: ON SELECTS "QUIET" MODE WHERE THE 5882EUH ONLY SENDS SIGNALS UPON ALARMS OR IF IT RECEIVES A SIGNAL FROM A 5839H KEYPAD. USE QUIET MODE FOR WESTERN EUROPEAN ETSI-300-200 COMPLIANCE.

OFF SELECTS NORMAL MODE. USE **OFF** POSITION IF 5839H IS PLUGGED INTO AN EXTERNAL POWER SOURCE OR IF A 5840H SIREN IS BEING USED.

5882EUH-US-001-V0

Figure 3-18a. 5882EUH Wireless Transceiver



5882eu_us

Figure 3-18b. 5882EU Wireless Transceiver

5839EU(H)/5882EU(H) Notes

- 5882EU(H) cover must be removed before enrolling 5839EU(H) keypad into receiver.
- Each 5839EU(H) can be enrolled in only one 5882EU(H) (do not assign a given 5839EU(H) to more than one transceiver).



Take note of the address you select for the wireless receiver as this address must be enabled in the system's *Device Programming* mode.

Installing the 5800TM Module

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

The 5800TM must be located between 0.3m and 0.6m from the receiver's antennas. The 5800TM must not be installed within the control cabinet. Mount the unit using its accompanying mounting bracket.

- Connect the 5800TM to the control panel's keypad connection terminals, using the supplied connector with flying leads, as follows:

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	

- Cut the red jumper for address setting 28; cut the white jumper for address 29; cut both jumpers for address 30.



This address must be enabled as an alpha keypad in the control's *Device Programming* mode and then assigned to a partition.

For additional information, refer to the 5800TM's instructions.

House ID Sniffer Mode

This mode applies only if you are using a wireless keypad (5827/5827AP/5827BD) in a 5800 series system. 5800 series receivers respond only to keypads set to the same House ID (01-31) that is programmed into the control panel. This prevents system interference from keypads in other nearby systems. 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, proceed as follows:

- Enter your "Installer Code" + [#] + [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**.
- To exit the Sniffer Mode, simply enter your Installer Code + OFF.



Since Sniffer Mode effectively disables wireless point reception, Sniffer Mode **cannot** be entered while any partition is armed.

5800/5800AP/5800EU/5800H Series Transmitter Setup

5800/5800AP/5800EU/5800H series transmitters have built-in serial numbers that must be "enrolled" by the system using the # 93 Menu mode programming, or input to the control via the downloader 5800/5800AP/5800EU/5800H series transmitters (except 5827/5827AP described separately) do not have DIP switches.

Each transmitter's zone number is programmed into the system in # 93 mode. Some transmitters, such as the 5816, 5816AP, 5816EU, 5816H and 5817, can support more than one "zone" (referred to as loops or inputs). On the 5816/5816AP/5816EU/5816H 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 and enrolled separately.

For button transmitters (wireless "keys"), such as the 5804, and, 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, which is automatically displayed when enrolled.

5800 Series Transmitter Supervision

Except for some transmitters that may be carried off-premises (5802, 5802AP, 5802CP, 5804, 5804AP, 5804EU, 5804BD, 5827, 5827AP), each transmitter is supervised by a check-in signal that is sent to the receiver at 70–90 minute intervals (25 minutes for 5800EU and 9 minutes for 5800H series). If at least one check-in is not received from each *supervised* transmitter within a programmed time period (i.e., 24 hours for 5800 or 2 hours for 5800EU/5800H), the "missing" transmitter number(s) and "CHECK" will be displayed.

The supervision for a particular transmitter that may be carried off the premises (5801, 5802AP, 5802MN, 5802MN2, 5802EU, 5802H) may be turned off by enrolling it as a "UR" (Unsupervised RF) type, as described later.

5800 series transmitters have built-in tamper protection and will cause a "CHECK" or "TRBL" condition to be annunciated if covers are removed, provided that program field *24 (Disable Expansion Zone Tamper) is set for "0." 5800EU series transmitters (5816EU, 5819EU, 5839EU and 5888EU) and 5800H series transmitters (5814H, 5816H, 5819H, 5819SH, 5839H, 5852H, and 5888H) are also tamper protected against wall removal.

5800 Series Transmitter Battery Life

Batteries in the wireless transmitters may last from 4-7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, temperature, as well as large swings in temperature may all reduce the actual battery life. The wireless system can identify a low battery situation when the battery still has 30 days of life remaining, thus allowing the dealer or user of the system time to arrange a change of battery and maintain protection for that given point within the system.

Some transmitters (e.g., 5802 and 5802CP) contain long-life but non-replaceable batteries. At the end of their life, the complete unit must be replaced (and a new serial number enrolled by the control).

Button type transmitters (ex. 5801, 5802, 5802AP, 5802CP, 5804, 5804AP, 5804H and 5804EU) should be periodically tested by the user for battery life.



Do not install batteries in wireless transmitters until ready to enroll them. This is to avoid interference. It is not critical to remove batteries after enrolling.

Compatible 5800 Series Transmitters

Model	Product	Input Type
5801	Panic Transmitter	UR or RF
5802	Pendant (Personal Emergency Transmitter)	BR Only
5802CP	Belt Clip (Personal Emergency Transmitter)	
5802MN/ 5802AP	Miniature (Personal Emergency Transmitter)	UR or RF
5802MN2	2-Button (Personal Emergency Transmitter)	UR or RF
5802EU/ 5802H*	2-Button (Personal Emergency Transmitter)	UR or RF
5804/ 5804AP	RF Key Transmitter	BR Only
5804EU/ 5802H*	RF Key Transmitter	BR Only
5804BD	RF Key Bi-directional Transmitter	BR Only
5806/ 5808LST/ 5808EU/ 5808H*	Photoelectric Smoke Detectors	RF
5816/ 5816AP	Door/Window Transmitter	RF
5816EU/ 5816H*	Door/Window Transmitter	RF
5816MN	Miniature Door/Window Transmitter	RF
5816TEMP	Temperature Sensor Transmitter	RF
5817	Multi-Point Universal Transmitter	RF
5818	Recessed Transmitter	RF
5819/ 5819EU/ 5819H*	Shock Sensor Analyzer Transmitter	RF
5819S/ 5819EUS/ 5819SH*	Shock Sensor Analyzer Transmitter	RF
5827/ 5827AP	Wireless Keypad	House ID
5827BD	Wireless Bi-directional Keypad	House ID
5849	Glassbreak Detector	RF
5852/ 5852H*	Glassbreak Detector	RF
5888EU/ 5888H*	PIR Detector	RF
5890	PIR Detector	RF
5890PI/ 5890AP	PIR Detector with Pet Immunity	RF

* CE approved and specifically type-approved in Finland, France, Germany, Italy, Netherlands, Norway, Portugal, Spain, Sweden, and Switzerland.

Installing Output Devices

The VISTA-120IT supports up to 96 outputs. Each device must be programmed as to how to act (ACTION), when to activate (START), and when to deactivate (STOP). The 4204, 4204CF, FSA-8/24, 4140SN and/or Powerline Carrier devices (i.e., X-10 brand devices) may be used.



The devices can be programmed to activate in response to a programmed **condition**. The system can also be programmed to activate these devices at specific **times** by using the #80 Scheduling Menu Mode–*Time Driven Events* function.

The 96 Output Devices may be supervised (zones 601-696). Only the relays on 4204CF modules may be supervised. If supervision is programmed for other types of Output Devices, unpredictable results may occur.

Wiring the 4204 Relay Module

- Set the 4204 DIP switches for a device address between 01-15 that is not being used by another device (keypads, RF receivers, etc.). If using more than one module, each module must be set to a different address.



The relay module will not operate until the device address you have chosen is enabled in the control's Device Programming mode.

- Connect the 4204 module(s) to the control's keypad terminals (6, 7, 8, and 9). Use the flying lead cable supplied with the relay module when mounting it in the control's cabinet. Use standard 4-conductor twisted cable when mounting the 4204 outside the cabinet.
- Directly wire each 4204 back to the panel. The maximum wire run length from the panel to the 4204 must not exceed:

Wire Size	Maximum Length
.64mm	38m
.81mm	60m
1.0mm	90m
1.3mm	150m

NOTE: DIP switch position 1
ON = enables tamper protection.
OFF = disables tamper protection.

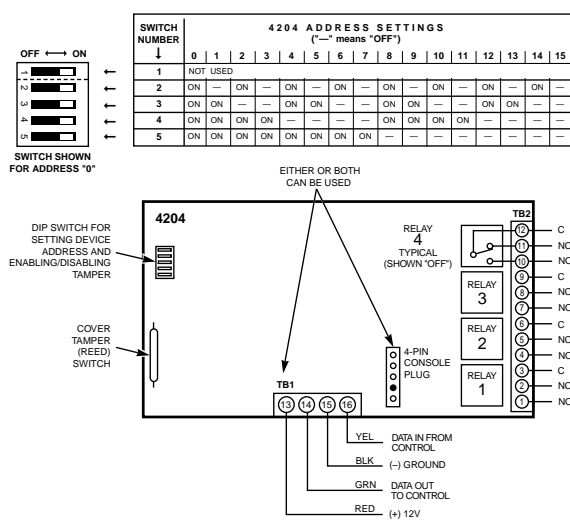


Figure 3-19. 4204 Relay Module

Installing Powerline Carrier Devices

If using 110VAC/60Hz 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. In Australia, use the XF10 and in Europe, use the XM10E in addition to the normal 16.5VAC/40VA output transformer.

X-10 Powerline Carrier devices are either plugged into standard AC outlets or wired into the AC electrical system by a licensed electrician, depending on the type of device used. They respond to "on" and "off" commands sent from the panel, through the 4300/XF10/XM10E, to the receiving devices. For more information about installing the transformer, see *Connecting the AC Mains Transformer* later in this section.

NOTE: If required, a low-pass filter (available from X-10) can be installed at the exit of the premises AC network to avoid possible conflict with nearby powerline carrier systems.

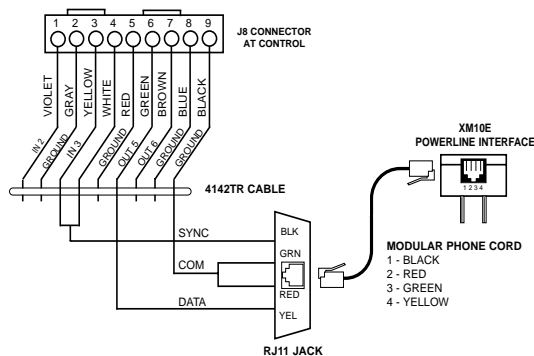


Figure 3-20. XM10E Modulator Connection

Installing the FSA Modules

The 8-zone LED Fire System Annunciator FSA-8 and 24-zone LED Fire System Annunciator FSA-24 enable a fire response unit to identify quickly 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.



The FSA 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, refer to *Figure 3-21* and perform the following steps:

Step	Action
1	Set the FSA's DIP switches for a device address from 08 to 23. See the module's instructions for the DIP switch table. Do not use an address 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).

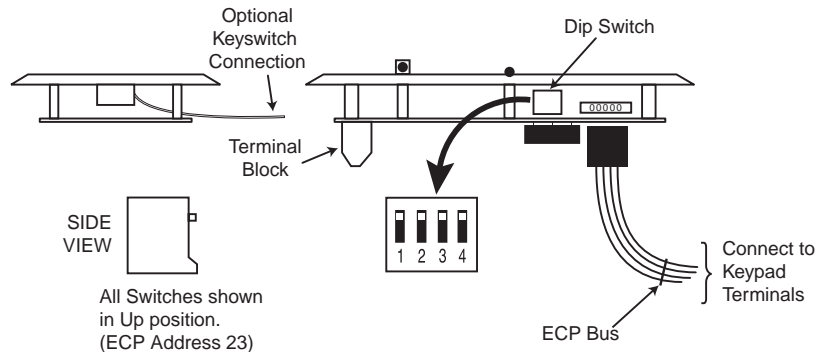


Figure 3-21: Wiring the FSA Module

Installing 4101SN Relay Modules

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

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



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

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

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

Open/Close Trigger Setup

Output 1 may alternately be programmed to change states when the system is armed in the away mode and then disarmed. If field 1*46 is set to 1, the output is set high when the system is in the "disarmed" state.

It switches to "0" volts when the system is armed in the "away" mode. This trigger will not change state unless *all* partitions are armed, and will change state again as soon as one partition is disarmed.

Installing a Remote Keypad Sounder

Output 1 may alternately be programmed for a remote keypad sounder. You may use an Amseco PAL 328N piezoelectric sounder for installations where you want the sounds produced by the keypad's built-in piezo sounder to be duplicated in another location for one partition. The panel will send all sounds remotely (i.e. alarm, trouble, chime, entry/exit, etc.) except for the short clicks associated with keypad key depression.

One application of this feature might be to produce chime sounds in a location that is distant from the panel's keypads. You can also accomplish this by using relay outputs (Refer to #93 Menu Mode Programming in the *Programming Guide*).

NOTE: Field *15 must be programmed with the partition number the remote sounder will duplicate

Connect the Amseco piezo between the panel's auxiliary power and the J7 connector trigger output as shown in the Remote Keypad Sounding Connections *Figure 3-22*.

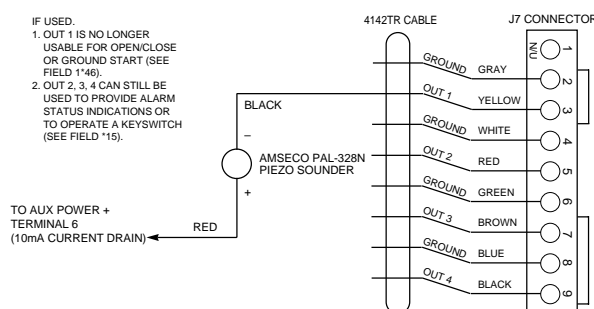


Figure 3-22. Remote Keypad Sounding Connections

Installing a Remote Keyswitch

If using an optional remote keyswitch for remote arming and disarming of the system, its switch must be connected to Zone 7 and its Ready and Armed status LEDs must be connected to the trigger outputs and programmed in order to become operational.



Note that a zone 7 keyswitch may be used in one partition only and Zone 7 is no longer available as a protection zone.

A momentary short across zone 7 will arm the partition in the "AWAY" mode. If the short is held for more than 3 seconds, the partition will arm in the "STAY" mode. After the partition has been armed, the next time Zone 7 is shorted, the partition disarms.

1. Connect the 4146 keyswitch's normally open momentary switch to Zone 7.
2. Connect a 2k EOL resistor across the switch regardless of whether or not zones 2-8 are selected to use EOL resistors.
3. Connect the keyswitch Armed and Ready LEDs to the J7 connector as shown.
4. Connect an optional closed circuit tamper switch (ex. No. 112) in series with zone 7.
5. Assign the keyswitch to its appropriate partition in program field *15. Enable open/close reporting (user #0) for the keyswitch in field *40 (if desired).

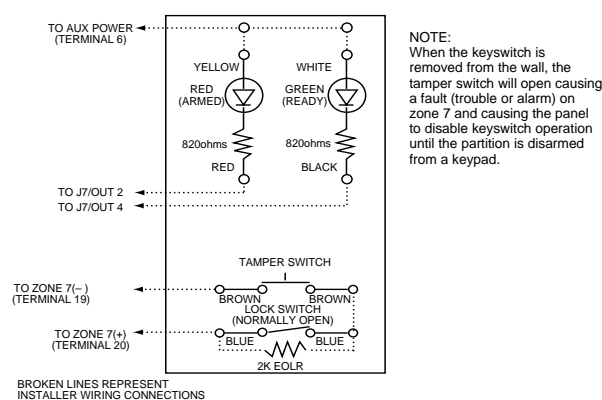


Figure 3-23. Remote Keyswitch Wiring

LED Indications

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

Keyswitch By Partition Configuration

In addition to being able to support a 4146 keyswitch on zone 7 of the control, you can add one keyswitch per partition via the use of a DPST or a DPDT keyswitch, wherein the key is removable in two positions: AWAY and OFF (disarm).

ADEMCO does not manufacture a packaged keyswitch with status LEDs (if status LEDs are desired, each must be driven by a programmed relay output). To use this configuration, connect each switch to ADEMCO's 4193SN 2-zone serial number RPM as shown below.

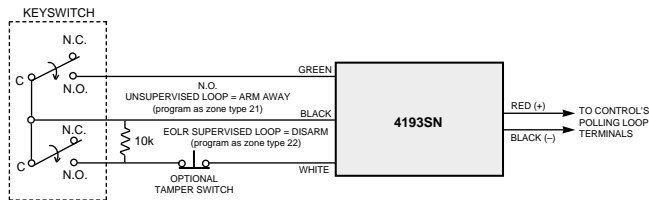


Figure 3-24. Keyswitch by Partition Wiring Connections

NOTE: The switch shown is Chicago Lock Company model EXA-112-2.

When the switch is NOT activated or is in the NC position, the partition is armed AWAY. When the switch is activated, the partition is disarmed. The unsupervised loop's zone must be assigned to zone type 21 (arm away) and the supervised loop's zone must be assigned to zone type 22 (disarm).

PROGRAMMING NOTE: Each zone of the 4193SN must be "enrolled" individually, but when the switch is turned, both zones activate. Therefore, before "enrolling" the serial number of a zone of the 4193SN, temporarily disconnect the wire from the side of the switch NOT being enrolled. After that zone is enrolled into the system, reconnect the wire, then temporarily disconnect the other wire to "enroll" the other zone.

Auxiliary Alarm Signaling Equipment

The J7 header provides triggers for fire, burglary/audible panic, silent/duress alarm. These triggers are programmed as the defaults for Outputs, 2, 3, and 4. These may be used to trip equipment such as Long Range Radios, Voice Diallers, Direct Wire Transmitters.

When used as alarm triggers, these outputs are normally low, and go high when the corresponding alarm condition occurs. These triggers remain high until the security code + OFF is entered at the keypad, with the exception of the Silent Panic/Duress trigger, which is a 2-second pulse.

The Figure 3-25 that follows shows how to make connections to the radio.



The triggers for Fire (Output 2) and Silent Panic/Duress (Output 4) may be used to operate keyswitch armed and ready LEDs *instead* when field *15 is enabled.

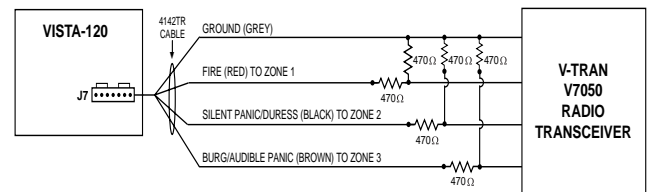


Figure 3-25. Auxiliary Alarm Signaling Equipment

Installing the VA8200 Panel Link Module

The VA8200 Panel Link Module (PLM) connects to the keypad (ECP) terminals on the VISTA-120IT and also connects to other PLMs via the RS-485 bus (3-wire twisted cable run). Figure 3-26 is a block diagram of a panel linking setup using three control panels.

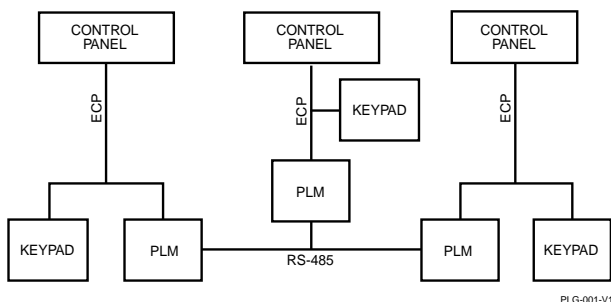


Figure 3-26: Panel Linking Block Diagram

ECP Wire Run Limitations

Determine wire size by referring to the table below.

Wire Run Length Table	
Wire Size	Length
0.64 mm	137m
0.81 mm	213m
1.0 mm	335m
1.3 mm	534m



- The length of the ECP wire runs combined must not exceed 610m when unshielded cable is used (305m if unshielded cable is run in conduit or if shielded cable is used).
- If more than one ECP device is wired to a single run, then the above maximum lengths must be divided by the number of devices on the run (e.g., the maximum length is 69m if two keypads are wired on a 0.64mm diameter wire run).

RS-485 Bus Wire Run Limitations

The RS-485 bus from the first Panel Linking Module to the last Panel Linking Module cannot exceed 1220m, using 1.3mm twisted-pair cable.

The recommended form of wiring is to daisy chain the connection from one unit to another. If several buildings are to be connected, the RS-485 bus should form a continuous path from one building to the next.

Avoid wiring units in a star configuration, where multiple branches are formed. Star configurations create loading and capacitance problems that are complex, and become difficult to troubleshoot.

Mounting and Wiring the Panel Link Module

The PLM will not operate until the device is enabled in the control's *Device Programming* in #93 Menu Mode. Do not mount the PLM on the cabinet door or attempt to attach it to the PC board.

To mount and wire the Panel Link Module, refer to *Figure 3-27* and perform the following steps:

Step	Action
1	Remove all power from the control panel before making any wiring connections.
2	Mount the module in the control cabinet if space is available or, adjacent to the cabinet, using 2-faced adhesive tape.
3	Set the PLM's DIP switches for a device address between 01 and 30. See the module's instructions for the DIP switch table. Do not use an address being used by another device (keypads, RF receivers, etc.).
4	Connect the 12V (+) and (–) and data-out and data-in connections from the PLM to the control's keypads terminals (6, 7, 8, and 9), respectively.
5	Connect the 3-wire RS-485 cable between each PLM. Recommended wiring is to bring the wires “in” from one module (or control panel) to terminals 5 (+), 6 (–), and 7 (G) and “out” to the next module from terminals TB1- 8 (+), 9 (–), and 10 (G).

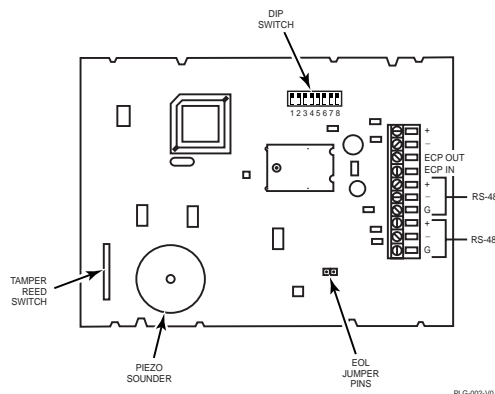


Figure 3-27: VA8200 Panel Link Module Wiring

Event Log Printer Connections

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

These categories are Alarm, Supervisory/Check, Bypass, Open/Close, and System Conditions.

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).

Printer Configurations

Printer must be configured as follows:

- 8 data bits, no parity, 1 stop bit
- 300 or 1200 baud (1200 preferred)
- Hardware handshaking using DTR signal

- The 4100SM module package includes a 3m RS232 cable. You can use a longer cable or an extension cable if the Control and serial printer are separated by more than 3m. The total cable length should be less than 15m.
- 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 does 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 Control will not send data to the printer unless the DTR signal is high.

Installing the 4100SM and the Printer

- Mount the 4100SM using its clip bracket to attach it to the side wall of the control cabinet.
- Make connections between J8, the 4100SM module and the serial printer as shown below. Connector J8, is located above connector J7 on the right side of the main PC board, and also provides triggers for powerline carrier devices.

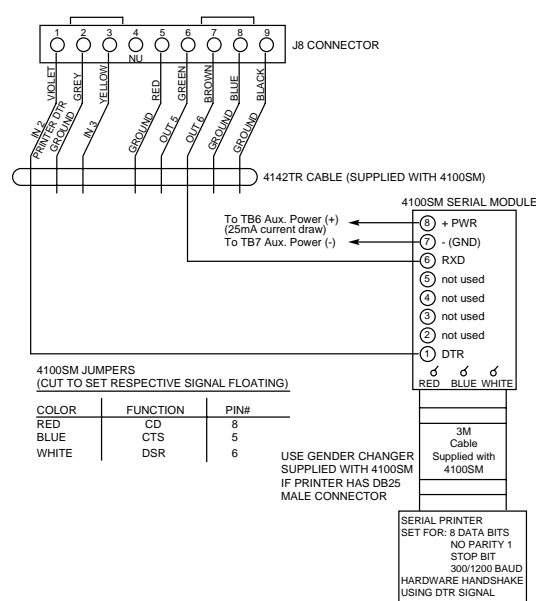


Figure 3-28. Event Log Printer Connections

Long Range Radio Connected to the ECP

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



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

Operation

The VISTA-120IT features **Dynamic Signaling Delay** and **Dynamic Signaling Priority** message reporting when Long Range Radio is used. These options are accessed through data fields ★56 and ★57, respectively. The Dynamic Signaling feature is designed to reduce the number of redundant reports sent to the central station.

The feature is described as follows:

Dynamic Signaling Delay (Field ★56)

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

Dynamic Signaling Priority (Field ★57)

Select the initial reporting destination for reports, Primary Dialer (0) or Long Range Radio (1).

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

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

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

Reports are transmitted from the VISTA-120IT to the LRR on a "first in/first out" basis. If events occur at the same time, they are transmitted in order of priority. The priority from most to least important is : Fire Alarms, Panic Alarms, Burglary Alarms, Fire Troubles, Non-Fire Troubles, Bypasses, Openings/Closings, Test messages, and all other types of reports.

There are two subscriber IDs programmed into the 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 is transmitted to both the primary and the secondary radio central stations before transmitting the second event.

If split reporting is selected for the VISTA-120IT, then the LRR will send the appropriate reports to the primary and secondary central stations.

Installing the ECP LRR

To install the ECP LRR, perform the following steps:

Step	Action
1	Mount the radio according to the instructions that accompany the radio.
2	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. See <i>Figure 3-29</i> .

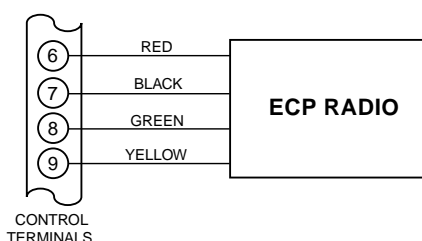


Figure 3-29: Wiring Long Range Radio to Keypad Terminals

Supervision

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

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

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

Trouble Messages

The following messages are displayed on the 6139/6160 when a problem exists on 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).

NOTES:

Items 2 and 3 require factory service.

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

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

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

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

Installing the 4286 VISTA Interactive Phone (VIP) Module

The 4286 VIP Module is an add-on accessory that permits the user to access the security system and relays via a DTMF multifrequency phone (either from the premises or by calling the premises from a remote location). This module must be enabled in *Device Programming* as device address 4, and must be assigned to a partition. Refer to #93 Menu Mode Programming in the Programming Guide.



Only one VIP Module can be used in a security system.

The 4286 VIP Module enables the user to do the following via a DTMF multi-frequency telephone:

- Receive synthesized voice messages over the phone regarding the status of the security system.
- Arm and disarm the security system and perform most other commands using the telephone keypad.

- Control 4204 relays and/or Powerline Carrier devices using the #70 relay mode.
- Provides voice annunciation over the phone to confirm any command that is entered.

NOTE: For languages other than English and/or where national telephone approvals are required, it is suggested that TeleCommand be used instead of the 4286.

Facts You Need to Know

- The VIP Module can announce many of the same words that would normally be displayed on a keypad under the same system conditions (see the words in **bold** in the Alpha Vocabulary list found in #93 *Menu Mode Programming* located in the *Programming Guide*). If the VIP module cannot annunciate a word in a zone descriptor, it will not annunciate the descriptor at all, but will still annunciate the zone number.
- Remote access to the VIP Module can be toggled on and off by using the [Security Code] + # 91 command (see VIP Module instruction manual). You must use the master or installer code only.
- The 4286 is wired between the control panel and the premises handset(s). It listens for multifrequency (DTMF) tones on the phone line and reports them to the control panel.
- During on-premises phone access, it powers the premises phones; during off-premises phone access, it seizes the line from the premises phones and any answering machines.
- The VIP Module reports trouble as zone 804 (800 + ECP device address 04 = 804) if data communication with the control is lost.
- 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 and Wiring the 4286 VIP Module

The VIP Module may be mounted in the control cabinet if space is available, or on the side of the cabinet or adjacent to it. Pry off the VIP Module's cover to wire.

1. When the VIP Module is mounted inside the control cabinet, attach it to the cabinet's interior surface with double sided adhesive tape. You may leave the module's cover off if it is mounted within the cabinet.



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

2. When mounting the VIP Module outside the cabinet, use the screw holes at the rear to mount horizontally or vertically (double sided 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).
3. Affix the 4286 connections label (supplied separately) to the inside of the VIP Module's cover

if the cover is used. Otherwise, affix the label to the inside of the *control cabinet's* door.

4. 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 below). These are the same connections as for remote keypads.

RED	6 (AUX +)
BLACK	7 (AUX -)
GREEN	8 (DATA IN)
YELLOW	9 (DATA OUT)

5. Insert the keyed connector at the other end into the mating header on the VIP Module.
6. Connect terminals 1 through 5 on the VIP Module as shown in *Figure 3-30*.



You must use an RJ31X jack with a direct-connect cord and make all connections **exactly** as shown. If the leads on the direct-connect cord are too short to reach their assigned terminals, splice additional wires to them, as required.

Terminal Block Connections

4286 Terminal	Connects to:
1. Phone In (Tip)	Terminal (26) on control.
2. Phone In (Ring)	Terminal (27) on control.
3. Phone Out (Tip)	BROWN lead from direct-connect cord.
4. Phone Out (Ring)	GREY lead from direct-connect cord.
5. Ground	Earth ground terminal (30) on control.
6. Audio Out 1	Speaker
7. Audio Out 1	Speaker

4286 WIRING NOTES:

- If multifrequency (DTMF) 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 & 4 on the 4286, **and** the pair of wires connected to terminals 26 & 27 on the control.
- Connection to the incoming telecom line via a RJ31X jack and direct-connect cord, as shown in this *Figure 3-30*, is essential, even if the system is not connected to a central station. **The 4286 will not function if this is not done.**
- The house phone lines must be connected to the VIP Module terminals **only!** If they are connected directly to the control panel or to the incoming line, an error tone will be heard when trying to access the VIP Module from an on-premises phone.
- If the telephone system on the premises includes a Caller ID unit, connect the unit directly to the "Handset" terminals (26 and 27) on the control.

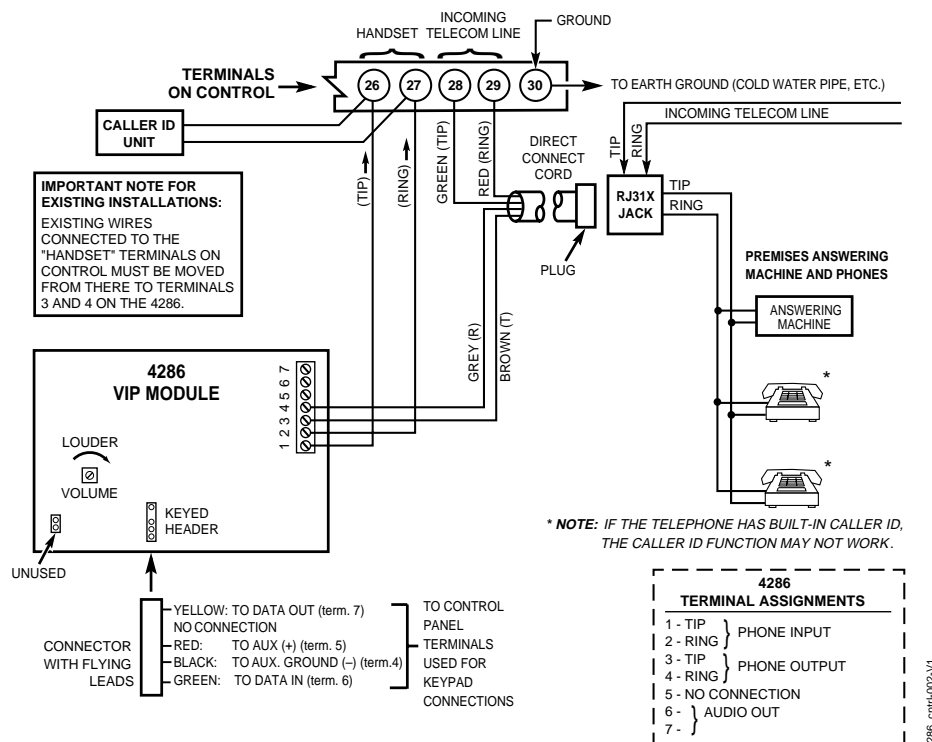
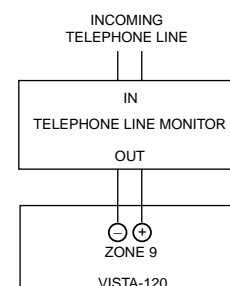


Figure 3-30. 4286 VIP Module Connections

Installing a Telephone Line Monitor

The VISTA-120IT supports the capability to monitor the telephone line for any wiring problems. This requires a separate module be connected between the telephone line and the control panel.

Follow the instructions accompanying the Telephone Line Monitor for installation of the monitor. Also, connect the output of the monitor to zone 9 on the control panel, see *Figure 3-31* and programme field 1*37 with a 1 (enable).



NOTE: PROGRAMME FIELD 1*37 WITH (1) ENABLE TO USE ZONE 9 FOR THE TELEPHONE LINE MONITOR INPUT

TLM-001-V0

Figure 3-31. Telephone Line Monitor Connections

Installing Audio Alarm Verification (AAV)

An Audio Alarm Verification (AAV) module (also known as two-way voice), such as the UVS-EU/UVS, is an add-on accessory that permits voice dialogue 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 for transmission to the primary phone number.

When using the AAV, zone 5 must be assigned a zone response type (e.g. response type 10), and option 1*60 and 1*66 must be selected as 1 to silence sounders on the premises. If these fields are not enabled, conversation with the premises will be difficult (too much noise on the premises). Note that zone 5 is no longer available as a protection zone.

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, and the cancel report field *81 is programmed as non-zero, 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 open for 1 minute.

Once triggering occurs, the control will give-up the phone line to the AAV module, without breaking the 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 if fields 1*60 and 1*66 are enabled. 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 phone connection and send the new fire alarm report, then re-trigger AAV mode. All other dialler messages triggered during on-going 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 3-32*. Field 1*46 can be used to set ground start, remote console sounding, or long range radio 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 as shown in *Figure 3-33*. If this method is selected, the START and STOP conditions for that relay must be set to choice 60 = "Audio Alarm Verification" during relay programming, via #93 *Menu Mode Programming* located in the *Programming Guide*.

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 4286 VIP/TeleCommand module remote access capability. The DIP switch settings shown on the triggering diagrams disable the remote AAV module trigger option. The control also requires that the AAV module trigger type is falling edge, which is set using the AAV's DIP switches.



1. 685 Receiver software must be rev. 4.6 or higher. Earlier versions will not hold the phone line connection open.
2. 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 to J7 connector trigger output, or to a 4204 relay module, as shown in the various AAV Connection diagrams that follow.



If also using a 4286 VIP Module, be sure to follow *Figure 3-34* when making connections.

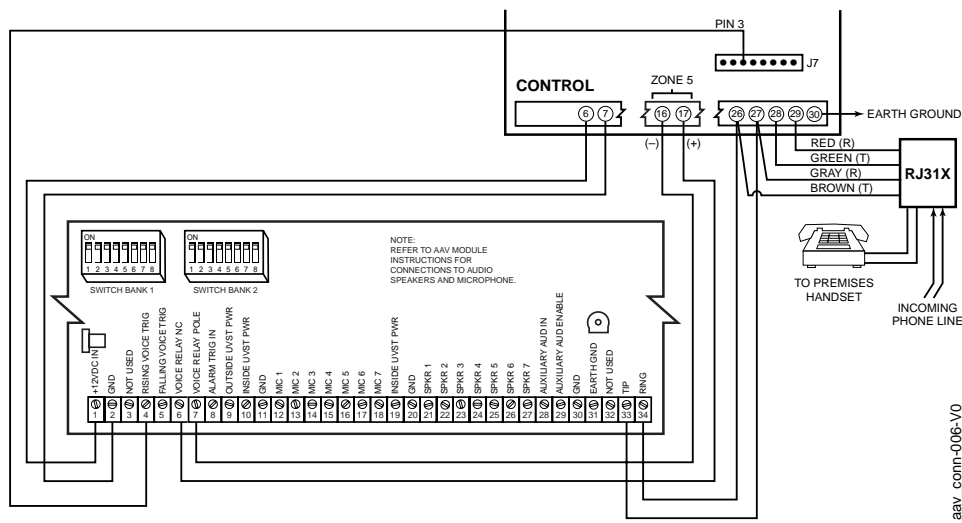


Figure 3-32. AAV Connections to Control Alone

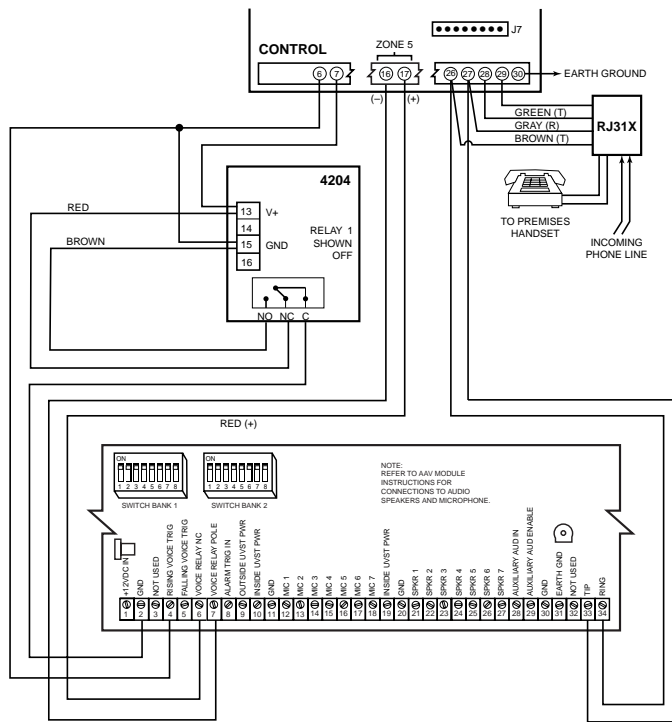


Figure 3-33. AAV Connections with a 4204

UVCM AND UVST SUMMARY OF CONNECTIONS

Refer to UVS Installation and Setup Guide K4214 for complete information.

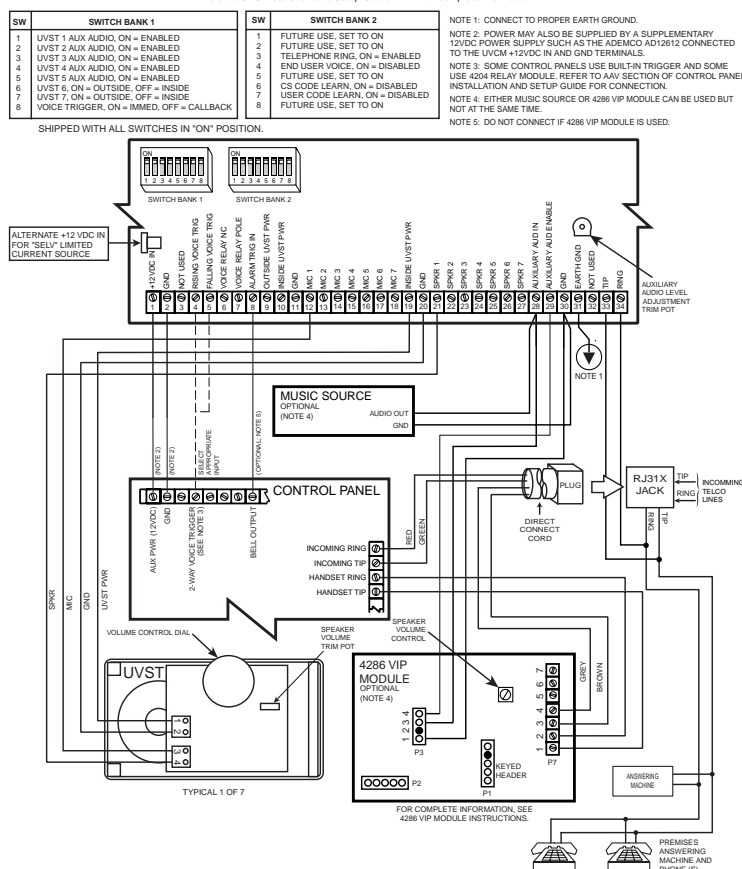


Figure 3-34. AAV Connections with a 4286

Video Alarm Verification (VAV)

This section provides only general information about the VAV option. Detailed information is in the manual provided with the VAV Transmitter.

A Video Alarm Verification (VAV) transmitter (e.g. VTP-50/Transpac receiver) is an add-on accessory that permits video imagery of the area where an alarm was detected to be transmitted on standard switched network telephone lines to the monitoring location using the same phone line and phone call on which the alarm is digitally communicated to the monitoring location.

The VAV transmitter connects to the control's handset telephone line (via a modem) and connects to 2 relays on a 4204 Relay Module: a "kissoff" relay, which signals the VTP-50 to begin communication, and a "hold the line" relay, which holds the phone line for 6 seconds to allow time for the VTP-50 to make connection to the Transpac receiver. In addition, a "camera" relay for each camera is used to trigger the cameras connected to the VTP-50.

VAV Operation

After all messages have been sent to the primary phone number during a reporting session, the control will transmit the VAV report (609) to a 685 (revision 4.73 or higher), which prepares the Transpac receiver to receive images. The “kissoff” relay activates, causing the VTP-50 to begin communication with the Transpac receiver, and the “hold the line” relay activates, giving the VTP-50 time to make connection to the Transpac receiver without breaking connection with the central station. The video image of the areas covered by the zones in the “camera” relay zone list is then transmitted to the Transpac receiver.

New alarms will automatically disconnect the video transmission and will be reported to the central station.

(Connection diagram is for reference only. Refer to the Summary of Connections diagram and the instructions accompanying the video transmitter being used for actual connections.)

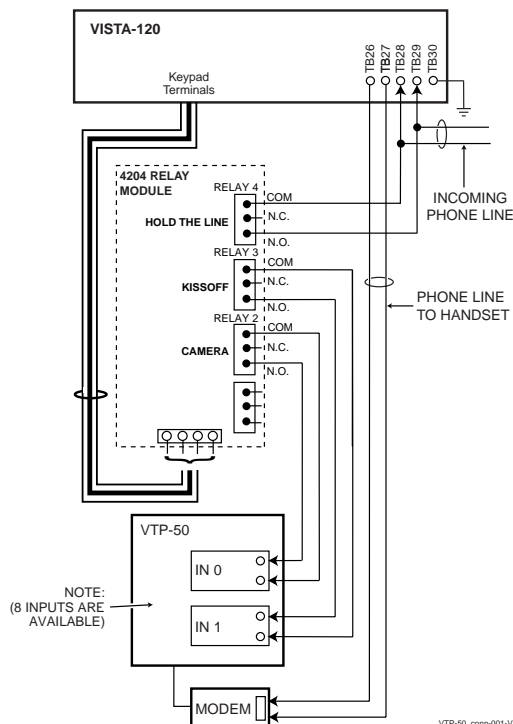


Figure 3-35. Connections to the Video Transmitter

Access Control Using ADEMCO VistaKey

VistaKey is a single-door access control module that, when connected to the VISTA-120IT provides access control to the protected premises. The alarm system can support up to 15 VistaKey modules (15 access points).



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

VistaKey Features

- Each VistaKey communicates with the VISTA-120IT via the V-Plex polling loop.
- In the event local power to VistaKey is lost, a VistaKey module provides backup monitoring of the access point door via a built-in Polling Loop device that is powered solely from the polling loop. It is programmed as a new type of Polling Loop device as part of the control's Polling Loop Device Programming. A serial number label is affixed to the VistaKey module for manual entry of its serial number.
- VistaKey supports up to 250 cardholders.
- The addition and removal of VistaKey modules from the system is easily accomplished via the VISTA-120IT keypad.

- All configurable options for each VistaKey are accomplished via software, firmware, and nonvolatile memory, eliminating the need for PC board jumpers, except assigning the access point zone number (1-15), which is set via a user-friendly, 16-position rotary switch.
- Each VistaKey provides one open-collector output trigger (sink 12mA @ 12VDC) and one Form C transfer contact relay.

Mounting and Wiring VistaKey



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

To mount and wire VistaKey, perform the following steps:

Step	Action
1	Mount the VistaKey, door strike or mag lock, and card reader.
2	Mount the door status monitor (DSM) and/or request-to-exit (RTE) devices.
3	Using <i>Figure 3-36</i> as a reference, connect the card reader interface cable to TB3, <i>making the +5V or +12V connection last.</i>

Step	Action
4	Connect the leads to TB1 in the following order: <ol style="list-style-type: none"> All ground leads to terminals 2, 5, and 9. The DSM, (optional) RTE, and General Purpose leads to terminals 6, 7, and 8, respectively. Door strike (or mag lock) lead to terminal 10. Local +12V or +24V supply lead to terminal 1. 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-120IT) to terminals 4 and 3, respectively.
6	Set the Address Select switch to the desired access door number (1-15).
7	Repeat steps 1 through 6 for each VistaKey being installed.

Connecting the Card Reader

Lead from Reader	Lead Color	To VistaKey TB3 Terminal #
Green LED	Orange	1
Ground*	Black	2
DATA 1 (Clock)	White	3
DATA 0 (Data)	Green	4
+5VDC†	Red†	6
+12VDC†	Red†	7

* TB-3 Terminal 5 is also a ground and may be used instead of terminal 2. Terminals 2 and 5 are a common ground.

† Connect to +5VDC OR +12VDC per reader manufacturer's specification.

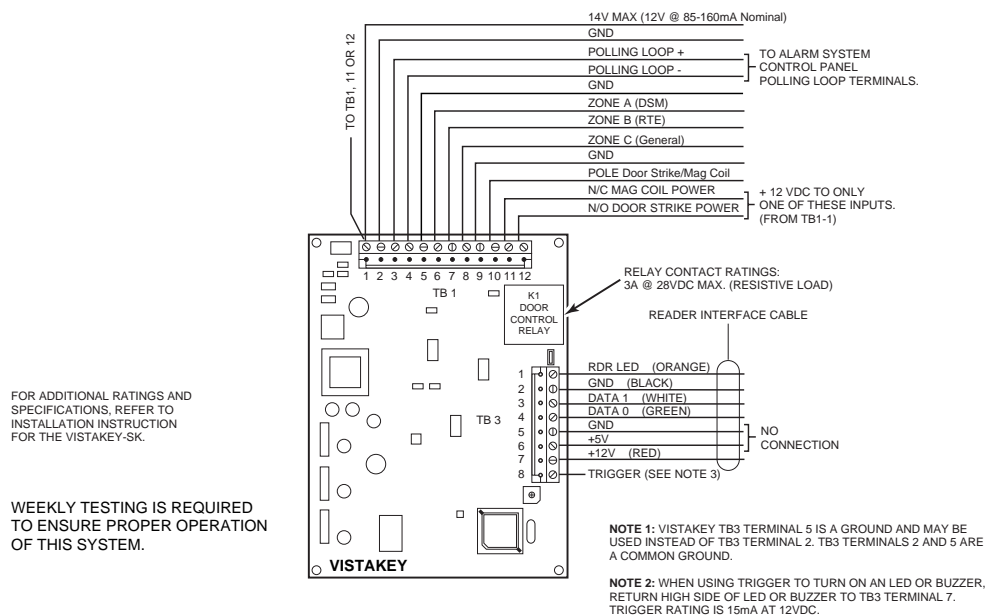


Figure 3-36: Wiring VistaKey

Access Control Using ADEMCO PassPoint ACS)

The VISTA-120IT interfaces with the PassPoint ACS via the VISTA Gateway Module (PTVGM). The PTVGM is connected between the ECP bus (keypad terminals) of the control and the network bus of the PassPoint ACS.

The control sends the PTVGM 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 PTVGM then reformats and retransmits this information to the Main Logic Board, (MLB) on the PassPoint ACS network bus.

Wiring the VISTA Gateway Module

The VISTA Gateway Module is connected between the ECP bus, (VISTA-120IT keypad terminals) and the network bus of the PassPoint Access Control System. See *Figure 3-37* for the proper wiring connections:

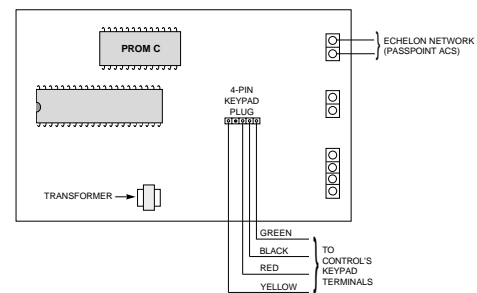


Figure 3-37. Wiring the VISTA Gateway Module

Connecting the AC Mains Transformer

This product uses the 1361 Transformer in 110 VAC markets. If you are using powerline carrier devices, use the 4300 Transformer. In Australia, use the XF10 and in Europe, use the XM10E in addition to the normal 16.5VAC/40VA output transformer.

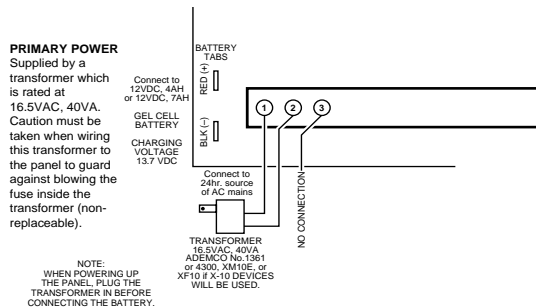


Figure 3-38. AC Mains and Battery Connections

Wiring the 1361 Transformer

Wire a 1361 110VAC Transformer (not supplied) to terminals 1 and 2 on the control panel as shown in *Figure 3-38*. In 220VAC regions, use a 16.5VAC/40VA output transformer.

Wiring the 4300/XF10 Transformers

Wire the 4300 Transformer as follows:

1. Connect terminals 1 and 3 (AC) and terminal 2 (Ground) of the 4300 transformer interface to control panel terminals 1, 2, and 30, respectively, see *Figure 3-39*.
2. Run a 6-conductor cable between the 4300 and the panel. Splice this cable to a 4142TR cable as shown below. Note that the white and yellow wires of the 4142TR **must be spliced** together.

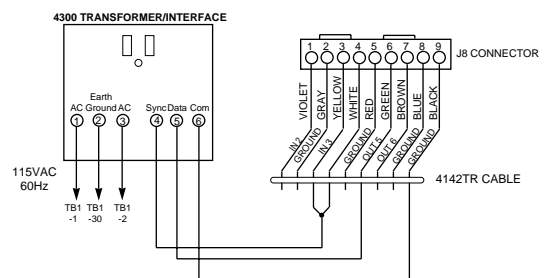


Figure 3-39. 4300 Transformer Connections

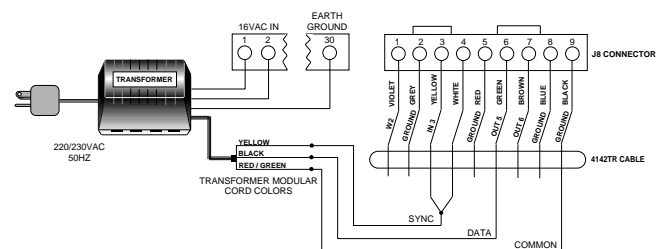


Figure 3-40. XF10 Transformer Connections

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. We recommend using 1.3mm diameter copper wire run at a maximum length of 7.5m. 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 power outlets only. To test the integrity of the ground terminal, use a three-wire circuit tester with neon lamp indicators.

Calculating the Battery Size Needed

In the event of an AC power loss, the Control panel will still operate for a period of time (time period varies depending on size of battery used) because the control has a back-up, rechargeable (sealed) lead acid battery. ADEMCO 467 (12V, 4AH) and ADEMCO 712BNP 12V, 7AH batteries are recommended.

The standby battery is automatically tested every 4 minutes for 13 seconds (or every 50 seconds for 1.5 seconds, as a function of program selection) and every 24 hours for 10 minutes, beginning 24 hours after exiting programming mode.

Use the following worksheets to calculate the total current drain on the control panel.

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

Table 1: Total Polling Loop Current Drain

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

* The total current cannot exceed 128mA. If total load exceeds 128mA, then a 4297 Loop Extender Module can be used. This module is powered from the panel's auxiliary power, and provides a separate polling loop output, which can support an additional 128mA load.

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

Table 2: Auxiliary Power Current Load

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

3. In Table 3, enter the total calculated subtotals from Tables 1 and 2, then add to get the total current.

Table 3: Total VISTA-120IT Standby Current Drain

	Total Standby Current	
Polling Loop Subtotal (see Table 1)		
Aux. Power Subtotal (see Table 2)		
Total Current Drain		

Use the following formula to calculate the battery size:

[Total Current Drain (Amps)] X [Number of Hours Standby Needed] = [Battery Ampere Hours].

Example: If the total current drain is 550mA (.55 Amps), and 24 Hr. standby is needed: $0.55 \times 24 = 13.2$ Ampere/Hour battery. In this example, two 7 Amp/Hr batteries connected in parallel must be used.

Installing The Back-Up Battery

1. Place the 12-volt back-up battery in the control cabinet.
2. Connect the Red battery wire to the positive (+) battery terminal **on the control board**.
3. Connect the Black wire to the negative (–) battery terminal **on the control board**.

NOTE: If two batteries are required, use the dual battery harness (supplied).

Programming

Program Modes

There are two programming modes for the VISTA-120IT. These are the Data Field Program Mode and the #93 Menu Mode. The Data Field Program Mode is where many system options are programmed. The #93 Menu Mode is an interactive mode that requires a 2-line alpha keypad.



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



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

Entering and Exiting Programming Mode

Enter Programming mode using either method a or b:

- Press both the [*] and [#] keys at the same time within 30 seconds after power is applied to the control.
- Enter the **Installer Code** + [8] + [0] + [0] + [0] keys. The factory installer code can be changed once in the Program mode (field *00).

NOTE: The default for the Installer Code is 4140.

Exit the Programming mode by either method a or b:

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

Data Field Programming Mode

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

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

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

SUMMARY OF DATA FIELD PROGRAMMING COMMANDS

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

Moving from One Page of Programming to Another

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

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

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

- Press *94.
- Press [*] + [XX], where XX = the last two digits of the program field, and make the desired entry.

NOTES:

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

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

Entry Errors

- If an address is improperly entered, the keypad displays “FC.”

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

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

Programming System-Wide Data Fields

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



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

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

- 1 Enter Program Mode: **Installer Code + 8 0 0 0**.

The following display appears:

Program Mode
* Fill # View – 00

- 2 If the control has not been programmed before, enter *97 to load factory defaults.
- 3 Press [*] and enter the first field number to be programmed (for example, *00, Installers Code). Make the desired entry. When the field is complete, the keypad beeps three times and advances to the next field. If you do not want to change the next field, press [*] and enter the next field number to be programmed.

First Page of fields
(*00 - *90)

To change to the next page of fields, press *94. To return to the previous page of fields, press *99.

- 4 Press *99 or *98 to exit Program Mode.

NOTE: If the number of digits that you enter in a data field is fewer than the maximum permitted (for

example, a phone number), the keypad displays the last entry and waits. To proceed, enter [*] + the next data field you wish to program.

Programming Partition-Specific Data Fields

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

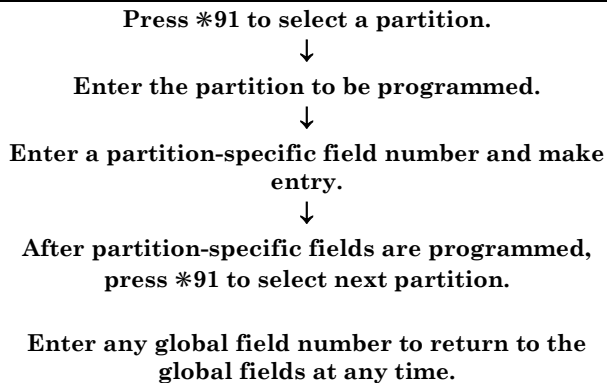
- 1 Enter Program Mode: **Installer Code + 8 0 0 0**.
- 2 Press *91, which will prompt you for the partition number desired.
- 3 Enter a partition-specific field number (e.g., *09) to begin programming.

When the first field's entry is completed, the next partition-specific field is automatically displayed. When all partition-specific fields are programmed, the system returns to the global programming fields (page 1 fields).

- 4 Repeat this procedure for each partition in the installation.

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

Programming Partition-Specific Fields



#93 Menu Mode Programming

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

Refer to the *VISTA-120IT Programming Guide* for detailed procedures for #93 Menu Mode Programming.

The following is a list of the main menu selections.

MAIN MENU	OPTIONS
ZONE PROG? 1 = YES 0 = NO 0	For programming the following: <ul style="list-style-type: none">• Zone Number• Zone Response Type• Partition Number for Zone• Dialler 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.

MAIN MENU	OPTIONS
-----------	---------

EXPERT MODE? 1 = YES 0 = NO 0	Same as Zone Programming except: <ul style="list-style-type: none"> • Done with a minimum number of keystrokes. • Can program wireless keys using pre-defined templates. NOTE: Some of the zone attributes cannot be programmed in the Expert Mode, only in Zone Programming.
REPORT CODE PROG? 1 = YES 0 = NO 0	For programming the following: <ul style="list-style-type: none"> • Alarm report codes for zones • Restore and supervisory codes • All other system report codes
ALPHA PROG? 1 = YES 0 = NO 0	For entering alpha descriptors for the following: <ul style="list-style-type: none"> • Zone Descriptors • Installer's Message • Custom Words • Partition Descriptors • Relay Descriptors
DEVICE PROG? 1 = YES 0 = NO 0	For defining the following device characteristics for addressable devices, including keypads, RF receivers (5881EN/5882EU/5882EUH/5882AP), 4204 relay modules, FSA (FSA-8/FSA-24), 4286 VIP Module, VA8200 Panel Linking Module, and VISTA Gateway Module: <ul style="list-style-type: none"> • Device Address • Device Type • Keypad Options (including Partition assignment) • RF House ID
OUTPUT PGM? 1 = YES 0 = NO 0	For defining output relay functions.
RLY VOICE DESCR? 1 = YES 0 = NO 0	For entering voice descriptors for relays to be used with the 4286 VIP Module. Note: Not applicable if using TeleCommand
CUSTOM INDEX ? 1 = YES 0 = NO 0	For creating custom word substitutes for VIP Module annunciation. Note: Not applicable if using TeleCommand
ACCESS POINT PGM 1 = YES 0 = NO 0	For defining the parameters for each of the VistaKey access points, including which group(s) have access through an access point (door). See the <i>VistaKey-SK Installation and Setup Guide</i> for the detailed programming instructions.
ACCESS GRP PGM 1 = YES 0 = NO 0	For defining the capabilities (privileges) for each group of users. See the <i>VistaKey-SK Installation and Setup Guide</i> for the detailed programming instructions.
EVENT/ACTION PGM 1 = YES 0 = NO 0	For defining events and time periods for an access group. See the <i>VistaKey-SK Installation and Setup Guide</i> for the detailed programming instructions.

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

#93 Menu Mode Programming Commands

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

Zone Index

VISTA-120 Installation and Setup Guide

The VISTA-120IT has 128 physical zones, as well as supervisory zones for relays, ECP devices (devices which communicate through the keypad terminals), and system troubles.

The zones are designated as follows:

Zone	Function
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	Basic Wired Zones
9	Telephone Line Monitor (if used)
1-128	5800 Series Wireless Devices
10-128	Polling Loop Devices
995	* + 1 Panic
996	# + 3 Panic
999	* + # Panic

ZONE # RANGE	ZONE FUNCTION	ACTUAL ZONE
001 - 128	Protection zones	As indicated
601 – 696	Relay Supervisory Zones	6 + 2-digit relay number (e.g. relay number 03, if supervised, is zone 603) NOTE: Relay supervision should be used only for relays on 4204CF modules.
800 - 830	ECP Device Supervisory Zones	8 + 2-digit Device Address, e.g., Device Address 01, if supervised, is zone 801. The 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 988: 2 nd Wireless Receiver – not receiving signals 990: 1 st Wireless Receiver – not receiving signals 997: Polling Loop (short circuit)
995, 996, 999	Keypad Panics	995: 1+□ panic (A key) 996: 3 + # panic (C key) 999: □ + # panic (B key)

NOTE: Zones 601 through 830, 988, 990, and 997 must be supervised and programmed with response type 05 (Day/Night) to comply with the “EN50131” specification.

Communication Programming Guide

Field #	Low Speed	Contact ID	High Speed	Express
*46, *48	Choose transmission speed and frequency	No effect	No effect	No effect
*52, *53	Send as either 4+2 or expanded	No effect	No effect	No effect
*79, *80	Enables alarm restores	Enables alarm restores	Enables alarm restores	Enables alarm restores
*49	Add checksum digit	No effect	Add checksum digit	No effect
*50	Sescoa/Radionics. Selects fixed digit time instead of fixed interdigit.	No effect	No effect	No effect

NOTE: Low Speed will **not** send 3+2 messages. Zone ID digit is suppressed.

Communication Defaults

*45	PRIMARY FORMAT	[1] ADEMCO Contact ID	*51	DUAL REPORTING	[0] no
*46	LOW SPEED FORMAT (Prim)	[0] ADEMCO Low Speed	*52	STANDARD/EXPANDED REPORT FOR PRIMARY	
*47	SECONDARY FORMAT	[1] ADEMCO Contact ID		[0] [0] [0] [0] [0] [0]	standard
*48	LOW SPEED FORMAT (Sec.)	[0] ADEMCO Low Speed		Alarm Rstr Bypass Trbl Opn/Cls Low Bat	
*49	CHECKSUM VERIFICATION	[0] [0]	*53	STANDARD/EXPANDED REPORT FOR SECONDARY	
	No checksum	Primary Secondary		[0] [0] [0] [0] [0] [0]	standard
*50	SESCOA/RADIONICS SEL.	[0] Radionics		Alarm Rstr Bypass Trbl Opn/Cls Low Bat	

Communication Defaults for Zones

ZONE #	1st	2nd	ZONE #	1st	2nd	ZONE #	1st	2nd	ZONE #	1st	2nd
1	01	00	37	05	00	73	01	00	109	05	00
2	02	00	38	06	00	74	02	00	110	06	00
3	03	00	39	07	00	75	03	00	111	07	00
4	04	00	40	08	00	76	04	00	112	08	00
5	05	00	41	01	00	77	05	00	113	01	00
6	06	00	42	02	00	78	06	00	114	02	00
7	07	00	43	03	00	79	07	00	115	03	00
8	08	00	44	04	00	80	08	00	116	04	00
9	01	00	45	05	00	81	01	00	117	05	00
10	02	00	46	06	00	82	02	00	118	06	00
11	03	00	47	07	00	83	03	00	119	07	00
12	04	00	48	08	00	84	04	00	120	08	00
13	05	00	49	01	00	85	05	00	121	01	00
14	06	00	50	02	00	86	06	00	122	02	00
15	07	00	51	03	00	87	07	00	123	03	00
16	08	00	52	04	00	88	08	00	124	04	00
17	01	00	53	05	00	89	01	00	125	05	00
18	02	00	54	06	00	90	02	00	126	06	00
19	03	00	55	07	00	91	03	00	127	07	00
20	04	00	56	08	00	92	04	00	128	08	00
21	05	00	57	01	00	93	05	00	601-696*	01	00
22	06	00	58	02	00	94	06	00	800-830*	01	00
23	07	00	59	03	00	95	07	00	970	00	00
24	08	00	60	04	00	96	08	00	988	02	00
25	01	00	61	05	00	97	01	00	990	04	00
26	02	00	62	06	00	98	02	00	992 (DURESS)	06	00
27	03	00	63	07	00	99	03	00	995	01	00
28	04	00	64	08	00	100	04	00	996	02	00
29	05	00	65	01	00	101	05	00	997	07	00
30	06	00	66	02	00	102	06	00	999	03	00
31	07	00	67	03	00	103	07	00	ALARM RST.	00	00
32	08	00	68	04	00	104	08	00	TROUBLE	00	00
33	01	00	69	05	00	105	01	00	TRBLE. RST	00	00
34	02	00	70	06	00	106	02	00	BYPASS	00	00
35	03	00	71	07	00	107	03	00	BYP. RST.	00	00
36	04	00	72	08	00	108	04	00			

* The programming of the first digit of each of these zones progresses in the same manner as the protection zones. For example, zone 601's first digit is 01; zone 602 is 02; zone 608 is 08; etc.

Zone Response Type Definitions

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

Type 00: Zone Not Used

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

Type 01: Entry/Exit #1 Burglary

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

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

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

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

Type 03: Perimeter Burglary

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

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

Type 04: Interior, Follower

Type 02: Entry/Exit #2 Burglary

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 AWAY or MAXIMUM, but the MAXIMUM mode eliminates the entry delay.

Interior Follower zone is automatically bypassed when the panel is armed in the STAY or INSTANT mode.

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

Type 05: Trouble by Day/Alarm by Night

Provides an instant alarm if the zone is faulted and the system is armed in the AWAY, STAY, INSTANT, or MAXIMUM mode. During the disarmed state (day), the system annunciates a latched trouble sounding from the keypad (and a central station report, if desired). There are programming options to prohibit bypass of this zone type except by installer and to prohibit restoration of the system (or partition) to the disarmed, ready to arm state subsequent to a trouble or alarm condition related to this zone type, except by the installer.

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. **This zone type should be assigned to system zones 601 to 830, 970, 988, 990, and 997 to comply with EN50131 specification.**

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/siren 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. (No 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/siren output. A zone of this type is always active and cannot be bypassed. **This zone type can be assigned to any wired zone except zone 9, and can be assigned to certain wireless system zones.**

Provides entry and exit delays (using the programmed entry and exit delay times) when armed in the AWAY mode. Provides only exit delay when armed in the MAXIMUM mode (no entry delay). Delay begins whenever sensors in this zone are violated, regardless of whether or not an entry/exit delay zone was tripped first.

The Interior with Delay zone is automatically bypassed when the panel is armed in the STAY or INSTANT mode.

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

Type 14: PLM Supervision

Provides supervision of remote Panel Link Modules. If the communication between the local PLM and a remote PLM fails, a trouble message is produced for the PLM zone.

Type 19: 24 Hour Trouble

An open or short on a zone with this zone type causes a trouble response. No external alarm sounders are activated.

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

Assign this zone type to an input device (wired zone, wireless zone, keypad, access control relay, etc.) that controls an access entry point (e.g., a door). The access point entry relay can be assigned to an access control relay (controlled by the VISTA-120IT), ECP relay (4204), or to the access control system independent of the VISTA-120IT.

Type 28: PassPoint Main Logic Board (MLB) Supervision

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

* Only use for 5800 series transmitters and polling loop RPMs connected to keyswitches.

Type 10: Interior with Delay.

Type 29: Momentary Exit

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

NOTE FOR PANIC KEYS: Keypad panic zones share the same zone response type for all 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 should be assigned zone type 05 if annunciation is desired.

Zone Input Type Definitions

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

Type 00 Not Used

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

Type 01 Basic Wired (HW)

This input type is reserved for the built-in basic wired zones 1-9.

Type 02 RF Motion (RM)

Select for 5800 Series RF transmitters. Sends periodic check-in signals, as well as fault and low-battery signals. The control panel automatically restores the zone to “ready” after a few seconds. This type is designed for facilities with multiple motion detectors that may fault and restore simultaneously. The transmitter must remain within the receiver’s range.

NOTE: Do not use this type with a door/window type transmitter.

Type 03 Supervised RF (RF)

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

Type 04 Unsupervised RF (UR)

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

Type 05 Unsupervised Button RF (BR)

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

Type 06 Serial Number Polling Loop (SL)

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

Type 07 DIP Switch Loop (DP)

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

Type 08 Second Loop Polling Loop (DS)

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

Type 09 Console Input (CS)

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

Type 10 PassPoint Access Control (ACS)

Select when this zone is mapped to a zone on the PassPoint Access Control System.

Type 11 VistaKey Door Status Monitor (DSM)

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

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

Type 12 VistaKey Request to Exit (RTE)

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

Type 13 VistaKey General Purpose (GP)

This input type operates in the same manner as other VISTA-120IT 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-120IT control panel.

Programming Access Control of an Entry/Exit Point

VistaKey

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

VistaKey Dialer Enables

When the VistaKey is installed with an alarm system, the system defaults are set so that the system does not send reports to the central station. The programming is accomplished in field 1*32 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.

PassPoint

The PassPoint ACS can dedicate some of its inputs for use as regular VISTA-120IT hardwired zones (the zone response type is ACS). The PassPoint ACS can also utilise the VISTA-120IT control panel dialler for reports to the central station.

Using ACS Zone Inputs

If the PassPoint ACS has uncommitted zones, these may be used by the VISTA-120IT as wired zones. To program for ACS zone inputs, perform the following steps:

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 the Programming Guide* for a detailed explanation.

PassPoint Dialler Events

All PassPoint ACS events can be sent to the VISTA-120IT dialler 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.

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 utilising keypads and button-type (BR) RF transmitters. A zone is programmed with a response type 27 (Access Point) and an appropriate input type (console, RF).

Using the Alpha Keypad

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

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

Using an RF Transmitter Zone

A button type RF transmitter (5804/5804AP/5804EU/5804H) 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 (5816/5816AP/5816EU/5816H) can be used with a remote switch to provide exit in case of a fire alarm using a PassPoint event action.

The PIR (5890/5890AP/5888EU/5888H) can be used to provide exit while preventing entry through a door.

The smoke detector (5808LST/5808EU/5808H) can be used to provide egress in emergency situations. To program the RF transmitter for access control, perform the following steps:

Step	Action
1	Enter Zone Programming in the #93 Menu Mode.
2	Program the zone with a response type 27 (Access Point).
3	Enter the access point number (00-31) of the door.
4	Indicate whether RF device is for entry or exit.
5	Enter the partition number
6	Enter the input type: button RF (05).
7	Enter the loop number.
8	Enroll the serial number

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



RF buttons and pendants must be assigned to a user number in order to function. See *SECTION 9: User Access Codes* for the procedure.

An RF transmitter will not provide access or grant if the system is in any test mode.

Using Wireless Keypads

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

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-120IT relays or the ACS relays or triggers are used with keypads and/or RF transmitters whose response type is Access Point (27).

To program the control of lighting and appliances, perform the following steps:

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

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

Using the VISTA-120IT for Stand-Alone Access Control

The VISTA-120IT can be used for access control without interfacing to PassPoint ACS or VistaKey. A user can trigger an access point (i.e., door strike) for 2 seconds by entering User Code + [0].

To program the VISTA-120IT for Stand-Alone access control, perform the following steps:

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

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

Programming for Panel Linking

Step	Action
1	Program the Panel Link Module (PLM) into the system in <i>Device Programming</i> in the #93 Menu Mode with Device Type 10.
2	If you want to supervise the PLM , program zone 8xx with response type 05, where “xx” = the module’s address. If you want the zone to report to the central station, make sure the report code for the zone is set with a non-zero value.
3	If you want to supervise the PLMs connected to other controls , program those modules in Zone Programming with response type 14. Also, program the panel ID number. The ID number must match the ID number programmed in <i>Device Programming</i> of the control panel the PLM is connected. If you want the zone to report to the central station, make sure the report code for the zone is set with a non-zero value. Be sure to program the input type with 00.

See Device Programming and Zone Programming in #93 Menu Mode Programming in the Programming Guide for a detailed explanation of the programming procedures.

Programming for the Video Alarm Verification

Program the 4204 relays as follows:

Device Type = 4
Relay Type = 1 (ECP)
ECP Address = (module's device address)
Relay Number = (actual relay number used on the module)

Relay "A" (kissoff):

action = 1 (closed for 2 seconds)
start zone type = 60 (alarm verification)
stop zone type = 60 (alarm verification)

Relay "B" (hold the line):

action = 2 (stay closed)
start zone type = 60 (alarm verification)
stop zone type = 57 (yyy seconds set in field 1*75; set to 6 sec.)

Relay "C" (camera):

action = 1 (closed for 2 seconds)
start event = 1 (alarm)
start zone list = "n" (zone list number containing camera zones for this relay)

Data Field Programming

*30 = (Multifrequency dialing)
*33 = primary phone number
*41 = 0 (use EOLR)
*45 = 1 (Contact ID)
*81 = enable cancel reports in order to send verification code (9th entry)
*84 = 00 (intermittent sensor disabled)
1*66 = 0 (disable silence of sounders during video alarm verification operation)
1*67 = 1 (must also be selected to assure that Contact ID report Event 609 will be transmitted to the monitoring location after the alarm transmission.)
1*75 = 006 (6 seconds)

NOTE: A zone list must be programmed which contains all zones protected by the camera being triggered by the "camera" relay.

Data Field Descriptions

About Data Field Programming

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

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



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

Programming Data Fields


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

FIELD	TITLE and DATA ENTRIES	EXPLANATION
*00	Installer Code Enter 4 digits, 0-9	The Installer Code is a 4-digit code reserved for installation company use. This is the only code that can be used to enter the Program Mode from the keypad. This code cannot be used to disarm the system if it isn't used to arm the system. This code cannot be used to re-enter Program Mode if Program Mode is exited by the *98 command.
*01	Master to Enable Installer 0 = disable 1 = enable	If enabled, the Master Code + OFF keying opens a 15-second time period in which the Installer Code can be used (Norwegian requirement).
*03	Final Contact Set 0 = disable 1 = enable	If enabled, the exit delay will be infinitely long and the system will arm 5 seconds after the Zone Type 01 exit door opens and closes or closes if already open and that condition was allowed prior to arming.
*04	Auto-bypass Exit Route Faults 0 = disable 1 = enable	If enabled, auto-bypass of unsealed burglary zones after 2 nd attempt to arm within 15 seconds after arming is rejected and the open zones are displayed (Swedish Requirement).
*05	Arm with Low Battery 0 = disable (ANPI requirement) 1 = enable	If enabled, the user can arm the partition or system with a system low battery present.
*06	Zone Type 5 Always Alarm 0 = disable 1 = enable	If enabled, a fault of a type 5 zone (tamper) causes a full alarm in any arming mode (disarmed or armed). If disabled, a fault of a type 5 zone (tamper) causes a trouble in the disarmed state and a full alarm in any armed state.
*07	Allow Arming With Faults in Exit Route 0 = disable 1 = enable	If enabled, allows arming with zone faults present in any of the exit route zones (zone types 1, 2, 4, and 10), wherein a fault remaining in any of these zone types at the end of the exit delay will result in a burglary alarm. (For STAY/INSTANT arming, this applies to zone types 1 and 2 only.) Automatic bypass of the zones is achieved (instead of alarm) if field 1*20 is also enabled.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*08	Self Activating Siren Output 0 = disable 1 = enable	If enabled, the alarm output is normally activated and turns off during alarms (ANPI requirement). If disabled the alarm output is normally off and turns on during alarms.
*09	Entry Delay #1 (partition-specific) Enter 01-15 multiplied by 15 seconds. 00 = no delay.	Entry delay defines the delay time that allows users to re-enter the premises through a door that has been programmed as an entry delay door and disarm the system without sounding an alarm. The system must be disarmed within this period or an alarm will occur.
*10	Exit Delay #1 (partition-specific) Enter 01-15 multiplied by 15 seconds. 00 = no delay.	Exit delay defines the delay period that allows users to leave the premises through a door that has been programmed as an entry/exit delay door after arming the system without setting off the alarm.
*11	Entry Delay #2 (partition-specific) Enter 01-15 multiplied by 15 seconds. 00 = no delay.	Entry Delay #2 is used for a secondary door requiring a longer delay than those assigned to Entry Delay #1.
*12	Exit Delay #2 (partition-specific) Enter 01-15 multiplied by 15 seconds. 00 = no delay.	Exit Delay #2 is used for a secondary door requiring a longer delay than those assigned to Exit Delay #1.
*13	Sounder Timeout (partition-specific) Enter 01-15 multiplied by 1 minute.	Defines the length of time the external sounder and the keypad's sounder will sound for all audible alarms. The timeout can be overridden by the Fire Timeout Disable option (field *21) for fire alarms.
*14	Zone 9 Response Time 0 = normal response (350msec) 1 = fast response (10msec)	If set for fast response, reacts to fast response devices connected to zone 9.
*15	Keyswitch Assignment Enter 1-8 partition keyswitch is being used. Enter 0 if the keyswitch is not used.	The keyswitch requires the use of zone 7 wired loop (zone 7 is no longer available as protection zone). The fire and panic alarm voltage triggers (J7) automatically become ARMING and READY status outputs for the Keyswitch LEDs. Zone type 10 is automatically assigned to zone 7 if a keyswitch is used. Openings/closing report as user "0" if enabled in field *40.
*16	Confirmation of Arming Ding (partition-specific) 0 = disable 1 = enable	If enabled, produces ½-second external alarm sounding ("ding") at the end of exit delay (or after kiss-off from the central station, if sending closing reports).
*17	AC Mains Loss Keypad Sounding 0 = disable 1 = enable	If enabled, sounding at the keypad (rapid beeping) occurs when AC power is lost (sounding occurs about 2 minutes after actual AC loss).
*18	Mains Presence Display 0 = disable 1 = enable	If enabled, displays AC presence (AC) in lower right-hand corner of keypad display.
*19	Randomise AC Mains Loss Report 0 = disable 1 = enable	If enabled, randomises AC loss reporting between 30 and 60 minutes after an actual AC loss. If disabled, AC loss reporting about 2 minutes after actual AC loss. Selecting this option helps prevent an overload of AC loss messages at the central station during a community blackout.
*20	Telephone Module Phone Code 1-9 = first digit of access code * or # = second digit of access code (enter # +11 for "*", or # +12 for "#") To disable enter 00 for the 1 st digit	If a 4286 Voice Module is being used, enter the 2-digit phone code used to access the system.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*21	Prevent Fire Timeout 0 = disable (timeout) 1 = enable (no timeout)	If enabled, there is no timeout of the alarm sounder duration for all fire zones, regardless of partition, so that fire sounding continues until the system is reset. If disabled, (timeout) the normal burglary sounder duration (field *13) applies to fire alarms.
*22	Keypad Panic Enables (partition-specific) 0 = disable 1 = enable	If enabled, the keypad panics (zones 995, 996, and 999) may be used in this partition. There are 3 entries in this field, one for each panic.
*23	Multiple Alarms (partition-specific) 0 = disable 1 = enable	If enabled, allows more than one alarm sounding for a given zone during an armed period. NOTE: that multiple alarm soundings will not occur more frequently than allowed by the programmed alarm sounder duration. This has no impact on the number of communication messages transmitted.
*24	Ignore Expansion Zone Tamper 0 = disable (tamper detection) 1 = enable (no tamper detection)	If disabled, the system monitors the tampers on expansion zones. NOTE: Only applicable to certain polling loop sensors with tamper switches or 5800 Series transmitters.
*25	Burglary Trigger for Response Type 8 0 = disable 1 = enable	If enabled, allows triggering of the voltage output on Pin 3 of the J7 header to include zone response type 8 (24-hr. auxiliary).
*26	Intelligent Test Report 0 = disable 1 = enable	If enabled, no test report is sent if any other type of report was sent since the last test report. If disabled, test reports are sent at the set intervals, regardless of whether or not any other report has been sent..
*27	Test Report Interval Enter 001-999 for the test report interval in hours. Enter 000 for test reporting.	If a test report is desired, enter a test code in field *81 and *82. Set first test report time in field *83.
*28	Power-Up in Previous State 0 = disable 1 = enable	If enabled, the system, upon power-up, reverts to its status prior to a complete power loss. If disabled, the system always powers up in a disarmed state. NOTE: Neither authority level 0 nor 5 can be used to disarm the system if the control powers up armed.
*29	Quick Arm (partition-specific) 0 = disable 1 = enable	If enabled, allows arming of the burglary system in AWAY, STAY, INSTANT, or MAXIMUM mode by using the [#] key instead of the user code. When armed, the system reports closing as User 0 if Open/Close reporting for User #2 (typically a Master level user) was enabled for a given partition. If Quick Arm is used, the Installer Code and Authority Level 5 codes cannot disarm the system.
*30	Multifrequency or Pulse Dial 0 = pulse 1 = multifrequency	Select the dialing method for the system
 <p>If you select multifrequency, make sure the subscriber has requested and is paying for multifrequency service. Note that whether or not multifrequency dialing for call placement is permitted, communication by the use of DTMF signaling (ADEMCO High Speed, 4 + 2 Express, ADEMCO Contact ID) will still take place. See field 1*33 for Multifrequency w/decadic dial pulse backup</p>		
*31	PABX Access Code Enter 00-09; B-F (11-15)	This field is used to enter up to four 2-digit numbers representing the prefix needed to obtain an outside telecom line. If not required, enter nothing and proceed to next field.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*32	Primary Subscriber's Account Number (partition-specific) Enter 00-09 ; B-F (11-15)	Enter a 3- or 4-digit (depending on report format) primary subscriber account number. Each number requires a 2-digit entry so as to allow entry of hexadecimal digits (B-F). If a 3-digit account number is to be used, enter data only in the first 3 locations, and enter * in the fourth location.
*33	Primary Phone Number Enter 0-9 ; #11 for *, #12 for #, #13 for a 2-second pause.	Enter the primary central station phone number, up to 17 digits. This is the phone number the control will use to transmit Alarm and status messages to the central station. Do not fill unused spaces. NOTE: Backup reporting is automatic only if a secondary phone number is entered.
*34	Secondary Phone Number Enter 0-9 ; #11 for *, #12 for #, #13 for a 2-second pause.	Enter the secondary phone number, up to 17 digits. The secondary phone number is used if communication on the primary number is unsuccessful, or if split/dual reporting is desired. Do not fill unused spaces. NOTE: If this field is programmed, a secondary subscriber account number (field *90) <i>must</i> also be programmed.
*35	Download Phone Number Enter 0-9 ; #11 for *, #12 for #, #13 for a 2-second pause.	Enter the downloading phone number, up to 17 digits. Do not fill unused spaces. NOTE: This field is applicable only if downloading is utilised.
*36	Download ID Number Make entries as 2-digit numbers as follows: 00=0 01=1 02=2 03=3 04=4 05=5 06=6 07=7 08=8 09=9 10=A 11=B 12=C 13=D 14=E 15=F	Enter eight digits. NOTE: This field is applicable only if downloading is utilised.
37	Download Command Enables 0 = disable 1 = enable	Enabling a function means that you are able to perform that function via the ADEMCO Compass Downloading software. Functions are as follows: Dialler Shutdown; System Shutdown; Restrict Access; Remote Bypass; Remote Disarm; Remote Arm; Upload Program; Download Program. *Restrict download access when the system is armed: can only arm unarmed partitions, upload program/event log, command relays and request status.
*38	Prevent Zone XXX Bypass (partition-specific) Enter a zone number (001-128). Enter 000 if all zones can be bypassed.	Enter three digits for zone that cannot be bypassed by the user. This selection does not affect fire zones, which the system prevents from being bypassed.
*39	Enable Open/Close Report for Installer Code (partition-specific) 0 = disable 1 = enable	If enabled, whenever the Installer Code is used to arm or disarm the partition, an open/close report is sent to the central station.
*40	Enable Open/Close Report for Keyswitch 0 = disable 1 = enable	If enabled, whenever the keyswitch is used to arm or disarm the partition, an open/close report is sent to the central station.
*41	Normally Closed or EOLR (Zones 2-8) 0 = EOLR used 1 = normally closed	If 0 , end-of-line resistors must be used on zones 2-8. If 1 end-of-line resistors cannot be used and only normally closed devices must be used.
*42	Suppress Fire Relay 0 = disable 1 = enable	If enabled, the system does not activate 4204/Powerline Carrier Device for fire alarms.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*43	Suppress Wireless Siren Activation for Fire Alarms 0 = disable 1 = enable	If enabled, the system does not activate wireless siren for fire alarms.
*44	Ring Detection Count Enter 00 to disable ring detection. Enter 01-14 for ring counts of 1-14. Enter 15 to select Answering Machine Defeat Mode	Only applicable if using a 4286 VIP Module, TeleCommand, and/or if remote-initiated downloading will be used. NOTES: Do not enter 00 if a 4286 or a TeleCommand is installed. In the Answering Machine Mode, the caller should let the phone ring once, then hang up, and call again within 30 seconds. The system, upon hearing one ring followed by nothing, does not answer the first call, but readies itself to pick up on the first ring of the next incoming call that is received within 30 seconds (i.e., the downloader calling again).
*45	Primary Format 0=Low Speed; 1=Contact ID; 2=ADEMCO High Speed; 3=ADEMCO Express	Enter the reporting format for the primary telephone number.
*46	Low Speed Format (Primary) 0 = ADEMCO Low Speed 1 = Sescoa/Radionics	Enter the low speed format for the primary telephone number.
*47	Secondary Format 0=Low Speed; 1=Contact ID; 2=ADEMCO High Speed; 3=ADEMCO Express	Enter the reporting format for the secondary telephone number.
*48	Low Speed Format (Secondary) 0 = ADEMCO Low Speed 1 = Sescoa/Radionics	Enter the low speed format for the secondary telephone number.
*49	Checksum Verification Enter 2 digits, one for the primary and one for the secondary. 0 = disable 1 = enable	If enabled, the system for either or both primary/secondary formats sends 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.
*50	Sescoa/Radionics Select 0 = disable 1 = enable	If enabled, selects Radionics, which uses hexadecimal 0-9, B-F reporting. If disabled, selects Sescoa, which uses only numeric reporting (0-9). NOTE: The selection applies to both primary and secondary phone numbers.
*51	Dual Reporting 0 = disable 1 = enable	If enabled, all reports are to be sent to both primary and secondary phone numbers. NOTE: If used with Split Reporting option 1 (1*34), alarms and restores go to both primary and secondary numbers, while all other reports go to secondary only. If used with Split Reporting option 2, alarms, restores and recent close go to both, open/close and test messages go to secondary only, while all other reports go to primary only. If used with Split Reporting option '3', alarms and restores go to both, all others go to the secondary only.
*52	Standard/Expanded Reporting Primary 0 = disable 1 = enable	This field has six entries as follows: Alarm, Restore, Bypass, Trouble, Open/Close, Low Battery. If enabled, expanded reports are sent to the primary phone number if low speed format is selected in field *45. NOTE: Expanded overrides 4+2 format.
*53	Standard/Expanded Reporting Secondary 0 = disable 1 = enable	This field has six entries as follows: Alarm, Restore, Bypass, Trouble, Open/Close, Low Battery. If enabled, expanded reports are sent to the secondary phone number if low speed format is selected in field *47. NOTE: Expanded overrides 4+2 format.
*54	Maximum Number of Dialler Attempts Enter (1-8).	Enter the number of attempts the dialler will attempt to communicate messages to the central station.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*55	Country Code 00 = Latin America, Spain, Italy, Eastern Europe, China 01 = Australia 02 = Belgium 03 = Denmark 04 = Finland 05 = France 06 = Netherlands 07 = Norway 08 = Sweden	Enter the country code to enable the proper telephone system for the dialler. NOTE: selections 01 – 07 require special hardware configuration.
*56	Dynamic Signaling Delay Enter 00-15 times 15 seconds.	Select the time the panel should wait for acknowledgment from the first reporting destination before it attempts to send a message to the second destination (first and second destinations are determined in field *57). NOTE: If the acknowledgment is received before the delay time expires, no message is sent to the second destination.
*57	Dynamic Signaling Priority 0 = Primary Dialer 1 = Long Range Radio	Select the initial reporting path for central station messages.
*58	Long Range Radio Central Station #1 Category Enable 0 = disable 1 = enable	Select which Contact ID messages will be transmitted on the Keypad bus for subscriber #1. The messages are as follows: Alarms, Troubles, Bypasses, Open/Close, System Conditions, Test Reports.
*59	Long Range Radio Central Station #2 Category Enable 0 = disable 1 = enable	Select which Contact ID messages will be transmitted on the Keypad bus for subscriber #2. The messages are as follows: Alarms, Troubles, Bypasses, Open/Close, System Conditions, Test Reports.
*60	Verified Alarm Report Enable 0 = disable 1 = enable	If enabled, a special Contact ID report is transmitted if 2 burglary alarms are detected within 45 minutes (Swedish requirement).
*61	Robofon Version of Contact ID 0 = disable 1 = enable	If enabled, the system uses Robofon version of Contact ID (Swedish requirement).
*79	Zone Type Restores for Zone Types 1-8 0 = disable 1 = enable	This field has eight entries, one for each zone type. Select the zone types that will send Restore reports.
*80	Zone Type Restores for Zone Types 9 and 10 0 = disable 1 = enable	This field has two entries, one for each zone type. Select the zone types that will send Restore reports.
*83	First Test Report Time Enter 00-07 for the day (01 = Monday) Enter 00-23 for the hour Enter 00-59 for the minutes	Enter the day and time that the first Test report shall be transmitted. Enter 00 in all locations if the Test report is to be sent immediately upon exiting. Enter 00 in the day location if the report is to be sent at the next occurrence of the time that is set.
*84	Intermittent Sensor Suppression (partition-specific) Enter 01-15 . Enter 00 for unlimited reports	This option limits the number of messages (alarms or troubles) sent for a specific channel in an armed period.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

*85	Enable Dialler Reports for Panics & Duress (partition-specific) 0 = disable 1 = enable	This field has four entries as follows: Zone 995, 996, 999, Duress Enable for each partition that the panics and duress reporting is desired.
*86	Report/Log Zone Type 23 0 = disable 1 = enable	If enabled, faults of zone type 23 are communicated and logged in the event log.
*87	Entry Warning (partition-specific) 0 = 3 short beeps 1 = slow continuous beeps	Select the type of warning for the entry delay period.
*88	Burglary Alarm Communicator Delay (partition-specific) 0 = no delay 1 = 30-second delay	Select the delay, if any, for burglary alarm communications.
*89	Restore Report Timing 0 = instant 1 = after siren timeout 2 = when system is disarmed	Select the time when restore reports are sent after an alarm.
*90	Secondary Subscriber Account Number (partition-specific) Enter 00-09; B-F (11-15)	Enter a 3- or 4-digit (depending on report format) primary subscriber account number. Each number requires a 2-digit entry so as to allow entry of hexadecimal digits (B-F). If a 3-digit account number is to be used, enter data only in the first 3 locations, and enter * in the fourth location. NOTE: This field <i>must</i> be programmed if a secondary phone number is used (field *34). This account number can be the same as the primary account number.
1*00	Contact ID Reporting in ASCII Through Printer Port 0 = printer – no ISDN 1 = ISDN + callout 2 = ISDN only 3 = callout if ISDN failed	Select the options for the printer port for event log printing.
1*01	ASCII Contact ID Reporting with or without ACK 0 = ACK required 1 = ACK not required	If you are using the printer port for printing of the event log, select if the ACK signal is required.
1*02	ASCII Contact ID Baud Rate 0 = 1200 1 = 2400 2 = 4800	Select the baud rate of the data on the printer port.
1*05	Bypass Enable for Fire Zones 0 = disable 1 = enable	If enabled, the system allows the bypassing of fire zones.
1*06	Suppress All Keypad Displays 0 = disable 1 = enable	If enabled, the system suppresses the displays of all keypads while the system is armed or disarmed. This includes alarms, troubles, etc. The suppression begins 2 minutes after a valid user code sequence is entered, (e.g., user code + OFF, user code + BYPASS, etc.). NOTE: If enabled, and an alarm or trouble occurs, these will display only after a valid user code + OFF is entered.
1*07	Check or TRBL Display 0 = CHECK 1 = TRBL	Select whether the system should display TRBL or CHECK for trouble conditions.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
-------	------------------------	-------------

1*08	Suppress Use of Armed LED on Keypads 0 = disable 1 = enable	If enabled, the system suppresses the armed LED when the system is in the armed state. This is for countries where the Red is only for indicating alarm.
1*09	Suppress Keypad Arming Status Indications When System is Armed 0 = disable 1 = enable	If enabled, the system suppresses all arming status indications when the system is armed. The suppression begins 2 minutes after a valid user code sequence is entered, (e.g., user code + OFF, user code + BYPASS, etc.). NOTE: If enabled, and an alarm or trouble occurs, these will display only after a valid user code + OFF is entered.
1*10	First to Alarm Display Lock 0 = scroll alarms 1 = lock display	If lock display is selected, the system displays of first fire alarm and requires the user to press the [*] key for a display of each additional fire alarm. Otherwise, the system automatically scrolls all fire alarms.
1*11	Common Area 1 Partition Enter 1-8 0 = none	Enter the common area 1 partition.
1*12	Affects Common Area 1 (partition-specific) 0 = disable 1 = enable	If enabled, causes common area 1 to disarm when this partition disarms. NOTE: This partition must be armed before common area 1 can be armed.
1*13	Arms Common Area 1 (partition-specific) 0 = disable 1 = enable	If enabled, arming this partition causes the system to attempt to arm common area 1 automatically. To enable this field, field 1*12 must also be enabled (partition-specific). NOTE: Common area 1 cannot be armed unless all partitions programmed for "affect" (field 1*12) are already armed.
1*14	Common Area 2 Partition Enter 1-8 0 = none	Enter the common area 2 partition.
1*15	Affects Common Area 2 (partition-specific) 0 = disable 1 = enable	If enabled, causes common area 2 to disarm when this partition disarms. NOTE: This partition must be armed before common area 2 can be armed.
1*16	Arms Common Area 2 (partition-specific) 0 = disable 1 = enable	If enabled, arming this partition causes the system to attempt to arm common area 2 automatically. To enable this field, field 1*15 must also be enabled (partition-specific). NOTE: Common area 2 cannot be armed unless all partitions programmed for "affect" (field 1*15) are already armed.
1*17	Common Area 3 Partition Enter 1-8 0 = none	Enter the common area 3 partition.
1*18	Affects Common Area 3 (partition-specific) 0 = disable 1 = enable	If enabled, causes common area 3 to disarm when this partition disarms. NOTE: This partition must be armed before common area 3 can be armed.
1*19	Arms Common Area 3 (partition-specific) 0 = disable 1 = enable	If enabled, arming this partition causes the system to attempt to arm common area 3 automatically. To enable this field, field 1*18 must also be enabled (partition-specific). NOTE: Common area 3 cannot be armed unless all partitions programmed for "affect" (field 1*18) are already armed.

Auto Bypass Logic

At the end of the exit delay, if a door is left open or an interior zone is faulted, the system starts the entry delay period, and sounds the bell/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 auto bypass occurs. If field *07 is enabled, the faulted zone(s) are auto bypassed at the end of

exit delay (no entry delay is activated). 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 dialler reports will be sent to the central station if programmed:

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

NOTE: If field *07 is enabled and field 1*20 is not enabled, then faults remaining in the exit route at the end of the exit delay will cause an immediate alarm. This report is programmed in data fields 1*40 and 1*41.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*20	Auto Bypass Faulted Exit Route Zones 0 = disable 1 = enable	If enabled, the system automatically bypasses any exit route zones that are faulted at the end of the exit delay. This field must be enabled if field *07 is enabled.
1*21	Exit Delay Reset 0 = disable 1 = enable	If enabled, when the panel is armed, the normal exit delay begins. After the user exits, closes the door, 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 again using the programmed exit delay time. NOTE: Exit Delay Reset is designed to allow an operator to re-enter the premises to retrieve a forgotten item without triggering an alarm.

Cross-Zoning

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

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

- Both zones in each set must protect the same area.
- When cross-zoning motion sensors, both device's areas of protection must be situated so that both units will trip at the same time if their shared protected area is violated.
- Both zones in each set must be in the same partition.
- A fire zone must only be crossed to another fire zone protecting the same physical area (**see following warning**).



DO NOT cross-zone a fire zone with a burglary zone under any circumstance. A fire zone must only be linked to another fire zone and BOTH must be protecting the same physical area (no walls or partitions separating them). As a guideline, we recommend that spacing between fire cross-zones be no further than 9m.

Conditions That Affect Cross-Zone Operation

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

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*22	Cross Zoning Pair One Enter 001-128 Enter 000,000 to disable	Select the first pair of cross zones, which must both be faulted within a five-minute period to cause an alarm.
1*23	Cross Zoning Pair Two Enter 001-128 Enter 000,000 to disable	Select the second pair of cross zones, which must both be faulted within a five-minute period to cause an alarm.
FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*24	Cross Zoning Pair Three Enter 001-128 Enter 000,000 to disable	Select the third pair of cross zones, which must both be faulted within a five-minute period to cause an alarm.

1*25	Cross Zoning Pair Four Enter 001-128 Enter 000,000 to disable	Select the fourth pair of cross zones, which must both be faulted within a five-minute period to cause an alarm.
1*26	Panic Button or Speedkey 00 = panic function (for D key = not used) 01-32 = macro number	Select for the A, B, and C keys whether the system performs a panic or a speedkey function when the key is pressed. Select for the D key whether the system performs a speedkey function or is not used.
1*27	Field 1*31 RF Transmitter Check-in interval to be Multiple of 1 Hour or 2 Hours 0 = 2-Hours 1 = 1 Hour	Select whether the programming of field 1*31 should be in 1 hour or 2 hour increments (must be 1 hour for CENELEC compliance).
1*28	RF Transmitter Low Battery Sound 0 = disarmed state only 1 = both armed and disarmed states	Select when the RF transmitter low-battery condition should display and audible beep annunciate on the keypad.
1*29	RF Transmitter Low Battery Reporting 0 = disable 1 = enable	If enabled, the system sends a Trouble message for RF transmitter low-battery condition to the central station. NOTE: The Trouble message will be sent for a transmitter supervision failure, independent of this selection.
1*30	RF Receiver Supervision Check-in Interval Enter 02-15 times 2 hours (4-30 hours). 00 = disable receiver supervision.	Select the check-in monitoring interval for the RF receiver(s). Failure of a receiver to receive any RF signal within the time entered results in the activation of the response type programmed for zone 990 for the first receiver and zone 988 for the second receiver and their related communication reports.
1*31	RF Transmitter Check-in Interval Enter 02-15 times 2 hours (4-30 hours). 00 = disable transmitter supervision.	Select the check-in monitoring interval for the RF transmitters. Failure of an individual transmitter to send a supervision signal within the time entered will result in a trouble response and related communication report.
1*32	Access Control Dialer Enables 0 = disable 1 = enable	There are six entries for this field as follows: Trace, Trouble, Not Used, Bypass, System, Alarm. If Trace is enabled, access grant/denial events are sent to the central station. For the other events, if enabled, a report is sent to the central station.
1*33	Multifrequency Dialling with Pulse Dial Back-up 0 = disable 1 = enable	If enabled, the communicator switches to decadic dial pulses if it is not successful on the first attempt using multifrequency.
1*34	Communicator Split Reporting Selection 0 = Split Reporting disabled 1 = Alarm, Alarm Restore, and Cancel reports to primary, all others to secondary 2 = Open/Close and Test reports to secondary, all other reports to primary 3 = Fire Alarms and Fire Restores to both, all other reports to secondary	Select the type of split reporting for system communication. NOTE: See *51 for split/dual reporting combinations.
1*35	Low Battery Test Interval 0 = 13 second test every 4 minutes (ANPI requirement) 1 = 1.5 second test every 50 seconds (Norwegian requirement)	Select the interval that the system performs a test of the system battery.
FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*36	CPU Fail Trigger Output 0 = disable 1 = enable	If enabled, output 2 on J7 to be CPU Fail output, overriding any other selection for output 2 (CENELEC requirement).

1*37	TLM Input on Zone 9 0 = disable 1 = enable	If enabled, the telephone line fault monitor is to be fed into zone 9. Note: The ADEMCO 659EN is a recommended telephone line fault monitor.
1*38	User Override of Tamper Alarms Instead of Installer Only Reset 0 = disable (ANPI requirement) 1 = enable	If enabled, allows the user to reset tamper alarms.
1*39	User Override of Tamper Faults Instead of Installer Only Bypass 0 = disable (ANPI requirement) 1 = enable	If enabled, allows the user to bypass tamper faults.
1*40	Maximum Number of Zones that can be Bypassed per Partition Enter 01-15 Enter 00 for no restriction	Select the maximum number of zones that can be bypassed for any armed period. This cannot be 00 for ANPI compliance.
1*41	Bypass/Unbypass Zones when Armed 0 = disable 1 = enable	If enabled, zones can be bypassed and unbypassed while the system is armed.
1*42	Call Waiting Defeat 0 = disable 1 = enable	If enabled, the system defeats Call Waiting on the first outgoing call attempt to both the primary and secondary numbers. NOTE: After the panel's initial call to report the alarm, the panel may attempt to make an additional call, perhaps for a cancel or a zone restoral. If Call Waiting is not defeated, an operator at the central station attempting to contact the premises (to verify whether the alarm is valid) hears the phone ringing indefinitely and must to dispatch on the call. DO NOT enable this feature unless Call Waiting is being used.
1*43	Permanent Keypad Display Backlighting (partition-specific) 0 = disable 1 = enable	If enabled, backlighting for the keypad display remains on at all times. Otherwise the backlighting comes on when a key is pressed. NOTE: When a key is pressed, display backlighting turns on for all keypads in that partition.
1*44	Keypad Tamper Detect 0 = disable 1 = enable (ANPI requirement)	If enabled, when 21 key depressions are entered, without a valid sequence (arm, disarm, etc.), the control panel disables all keypads in that partition. This includes any wireless keypads. After 15 minutes the inhibit is automatically removed.
1*45	Exit Delay Sounding (partition-specific) 0 = disable 1 = enable	If enabled, the system produces slow beeping from the keypads during exit delay and reverts to rapid beeping during the last 10 seconds of the exit delay.
1*46	Auxiliary Output Mode 0 = ground start output. 1 = smoke detector reset. 2 = keypad sounds at an auxiliary sounder. 3 = AAV module.	Select the mode for output 1 on the J7 triggers. NOTES: Only one of the options may be active within the system. Option 2 applies only to the partition enabled in field *15.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*47	Chime on External Siren (partition-specific) 0 = disable 1 = enable	If enabled, the system produces chime annunciation on the external alarm sounder.

1*48	Wireless Keypad Assignment 0 = none 1-8 = partition number	Select the partition in which 5827/5827BD RF keypad is used.
1*49	Suppress Transmitter Supervision Sound 0 = disable 1 = enable	If enabled, no trouble soundings occur on the keypad for transmitter check-in failures.
1*50	Number of Seconds Added per Day Enter 00-30	Enter the number of seconds that will be added per day to correct the real-time clock, if internal crystal synch is selected in 1*54.
1*51	Number of Seconds Subtracted per Day Enter 00-30	Enter the number of seconds that will be subtracted per day to correct the real-time clock, if internal crystal synch is selected in 1*54.
1*52	Send Cancel If Alarm + Off (partition-specific) 0 = disable 1 = enable	If enabled, Cancel reports are sent when the system is disarmed after an alarm, regardless of how much time has gone by. If disabled, Cancel reports are sent within Alarm Sounder Timeout period only.
1*53	Disable Download Callback 0 = callback required 1 = no callback required	Select whether a callback from the control panel is required for downloading.
1*54	Internal Clock Sync 0 = use AC sync for clock 1 = use internal crystal for clock	Select the sync method for the real-time clock.
1*55	International Date Format 0 = disable (mm/dd/yy) 1 = enable (dd/mm/yy)	Select the date format for display in the event log.
1*56	AC 60Hz or 50Hz 0 = 60Hz 1 = 50Hz	Select the frequency for the AC mains.
1*57	Enable 5800 RF Button Global Arm 0 = disable 1 = enable	If enabled, the system arms/disarms in accordance with the button's user's global arming settings.
1*58	Enable 5800 RF Button Force Arm 0 = disable 1 = enable	If enabled, allows the RF button user to force a bypass of all faulted zones when arming the system. NOTE: When attempting to arm the system, the keypad beeps once after the button is pressed if any faulted zones are present. The user should then press the button again within 4 seconds to force-bypass those zones and arm the system.
1*59	Suppress Status LED Output When Zone 7 Keyswitch Enabled/Retain Voltage Trigger Outputs 0 = disable 1 = enable	If enabled, the system suppresses the keyswitch status LEDs and provides voltage triggers on the J7 outputs.
FIELD	TITLE and DATA ENTRIES	EXPLANATION
1*60	Zone 5 Audio Alarm Verification 0 = disable 1 = enable	If enabled, zone 5 is used for 2-way audio (AAV). NOTE: Zone 5 cannot be used as protection zone.
1*61	Display Tamper 0 = disable 1 = enable	If enabled, the system displays "Tamper" instead of "Check" or "Trbl" (see field 1*07).

1*62	Tamper Detect in Test Mode 0 = disable 1 = enable	If enabled, the system terminates the test mode and displays the tamper condition. If disabled, the system remains in test mode and displays "fault."
1*66	Silence Sounder During AAV 0 = disable 1 = enable	If enabled, the system silences the alarm sounder and the keypad when AAV is being used and listening microphones are on.
1*67	Video Alarm Verification 0 = disable 1 = enable	If enabled, the system transmits the Contact ID code 609 so the central station equipment can be ready for video image reception and processing.
1*70	Event Log Types 0 = disable 1 = enable	This field has five entries as follows: Alarm, Check, Bypass, Open/Close, System. If enabled, the system logs those types of events into the event log. NOTE: Events are also logged into the PassPoint system, if installed.
1*71	12/24 Hour Time Stamp Format 0 = 12-hour 1 = 24-hour	Select the type of time stamping for the event log.
1*72	Event Log Printer On-Line Mode 0 = disable 1 = enable	If enabled, the system prints the events as they occur. If disabled, the system prints the log only upon request.
1*73	Printer Baud Rate 0 = 1200 (preferred) 1 = 300	Select the baud rate for the serial printer.
1*74	Relay Timeout XXX Minutes Enter 000-127 times 2 minutes (000-254).	This is used for #80 Menu Mode Time-Driven event relay command numbers "04/09" and <i>Output Programming</i> in the #93 Menu Mode Programming output command "56."
1*75	Relay Timeout YYY Seconds Enter 000-127 seconds.	This is used for #80 Menu Mode Time-Driven event relay command numbers "05/10" and <i>Output Programming</i> in the #93 Menu Mode Programming command "57."
1*76	Access Control Relay (partition-specific) 01-96 = relay number 00 = relay not used.	If enabled, the assigned relay closes for 2 seconds when the user enters his code and presses 0.
1*77	Log First Maintenance Signal 0 = no logging 1 = log first maintenance signal from each smoke detector	Select whether the system should log the first maintenance signal from each smoke detector.
2*00	Number of Partitions Enter 1-8.	Enter the number of partitions used in the system.

FIELD	TITLE and DATA ENTRIES	EXPLANATION
2*01	Summer Time Start/End Month 0 = disable 1 = enable	Enter the months (00-12) in which summer time starts and ends. Enter 00, 00 if summer time does not apply to the user's region. Standard setting for North America is 04,10. NOTE: Summer time starts and ends at 2AM on the designated month and weekend
2*02	Summer Time Start/End Weekend 0 = disable 1 = enable	Enter the start and end weekends for summer time as follows: 1=first; 2=second; 3=third; 4=fourth; 5=last; 6=next to last; 7=third from last. Standard setting for North America is 1,5.

2*05	Auto-Arm Delay (partition-specific) 00 = no delay 01-14 times 4 minutes (04-56) delay 15 = no auto arming	This is the time between the end of the arming period and the start of auto-arm warning time (field 2*06).
2*06	Auto-Arm Warning Period (partition-specific) 01-15 times 1-minute warning 00 = no warning period	This is the time that the user is warned by a keypad sounding and display to exit the premises prior to auto arming of the system.
2*07	Auto-Disarm Delay (partition-specific) 00 = no delay 01-14 times 4 minutes (04-56) delay 15 = no auto disarming	This is the time between the end of the disarming time period and the start of auto disarming of the system.
2*08	Enable Force Arm for Auto-Arm (partition-specific) 0 = disable 1 = enable	If enabled, the system automatically bypasses any faulted zones when it attempts to auto-arm. If disabled, the system will not auto-arm.
2*09	Open/Close Reports by Exception (partition-specific) 0 = disable 1 = enable	If enabled, Open/Close reports are sent only if the openings/closings occur outside the arm and disarm time periods. NOTES: Open reports are also suppressed during the closing time period in order to prevent false alarms if the user arms the system, then re-enters the premises, for example to retrieve a forgotten item. Openings and closings are still recorded in the event log. 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 = disable 1 = enable	If enabled, disarming of the system is allowed only during the arming/disarming time periods, or if the system is in alarm (if 2*11 is set to 1). NOTE: This applies only to Operator-level users. Installer, Master, and Manager-level users can disarm the system at any time.
2*11	Allow Disarm Outside Window if Alarm Occurs 0 = disable 1 = enable	If enabled, allows the system to be disarmed outside the programmed disarm (opening) time period if an alarm has occurred. Otherwise disarming is allowed only during the disarm time period. NOTE: Used only if field 2*10 is enabled.
2*18	Enable GOTO for this Partition (partition-specific) 0 = disable 1 = enable	If enabled, this partition can be accessed from another partition's keypad using the GOTO command.
2*19	Use Partition Descriptors 0 = disable 1 = enable	If enabled, the normal keypad display will include a partition number and four-digit descriptor.
FIELD	TITLE and DATA ENTRIES	EXPLANATION
2*20	Enable J7 Triggers for Partition (partition-specific) 0 = disable 1 = enable	If enabled, the J7 triggers function for this partition.
2*21	Supervision Pulses for LRR 0 = disable 1 = enable	There are three entries in this field as follows: Fire, Burglary/Audible Panic, Silent Panic/Duress. If enabled, causes the control to send periodic short pulses on the J7 radio triggers to the LRR. The LRR uses these pulses to determine that its connection to the control is still intact.

2*22	Display Fire Alarms of Other Partitions (partition-specific) 0 = disable 1 = enable	If enabled, allows fire alarms that occur on other partitions to be displayed at this partition's keypad(s).
2*23	Display Burglary & Panic Alarms for Other Partitions (partition-specific) 0 = disable 1 = enable	If enabled, allows burglary and panic alarms that occur on other partitions to be displayed at this partition's keypad(s).
2*24	Display Troubles of Other Partitions (partition-specific) 0 = disable 1 = enable	If enabled, allows troubles that occur on other partitions to be displayed at this partition's keypad(s).
2*25	Override AC/Comm Fail 0 = disable 1 = enable	If enabled, allows the arming of the partition or system with an AC Loss or Communication Failure present on the system.

Scheduling Options

Introduction To Scheduling

General

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

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

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

Auto Arming

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

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 period 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 period.

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

Auto-Arm Warning

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

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

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

Force Arm

The Force Arm option causes the panel to attempt to bypass any faulted zones prior to auto arming (panel performs a force-arm). This option is set in partition-specific program field 2*08.

Extend Closing Time Period

A user can manually delay the arm (closing) time period 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 time periods begin at the end of the extension.

Auto Disarming

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

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 period.

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 period and during the arming time period (in case user needs to re-enter premises after manually arming the partition).

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

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 period.

Time-Driven Events

By using the time periods, 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 period:

- At the beginning of a time period
- At the end of a time period
- During a time period (on at beginning of time period, off at end)
- At both the beginning and end of the time period (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 (e.g., turn on the porch light this Wednesday at 2000).

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 is inactive.

The system provides up to 8 access schedules, each consisting of two time periods (typically one for opening, one for closing) for each day of the week and two time periods 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 the schedule, the alpha keypad displays “Access Denied.”

Time Period Definitions

Scheduled events are based on time periods, which are simply periods of time during which an event may take place.

The system supports up to 20 time periods, each defined by a “Start” time and a “Stop” time.

The time periods 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	0900 to 1800
Friday	0900 to 2100
Saturday	1000 to 1600
Sunday	Closed
Holidays	Closed

Assume the owner desires the following time periods to allow time for employees to arm or disarm the system:

Monday to Thursday	Open (disarm)	0800 to 0900
	Close (arm)	1800 to 1830
Friday	Open (disarm)	0800 to 0900
	Close (arm)	2100 to 2130
Saturday	Open (disarm)	0900 to 1000
	Close (arm)	1600 to 1630
Sunday & Holidays	Closed	

To provide these schedules, the following five time periods need to be programmed:

Time Period	Start	Stop	Purpose
1	0800	0900	Monday-Friday open time period
2	0900	1000	Saturday open time period
3	1600	1630	Saturday close time period
4	1800	1830	Monday-Thurs. close time period
5	2100	2130	Friday close time period

Using the #80 Menu Mode (described later in this section), the installer can program open/close schedules by assigning each time period to a day of the week (time periods 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 periods 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 period for openings and one time period 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 time period and one closing time period per day.

Holiday Schedule

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

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

Temporary Schedule

The temporary schedule provides a method for the end user to override the daily and holiday schedules. It consists of one opening time period and one closing time period 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 period. Reports are only sent if the arm or disarm occurs outside the assigned time period.

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

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

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

Example of Open/Close Exception Reporting & Scheduling

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

1801	0559	0600	0900	0901	1559	1600	1800	1801	0559
Early Opening reports are sent if system is manually disarmed before opening time period begins. Early and Late Opening and Closing reports are programmable options in the Report Code Programming. They are not dependent on the programming of the Exception Reporting option.		<div>Opening Window</div> <p>No reports are sent if system is disarmed during this time period.</p> <p>If an arming occurs, a Closing report is sent to the central station regardless of how the Exception Reporting option is set.</p>		Auto-disarm delay begins. Auto-disarm occurs after delay (if auto-disarm is enabled). Missed Opening reports are sent if manual disarming has not occurred at expiration of opening time period. Late Opening reports are sent if disarm occurs after the opening time period expires. Early Closing reports are sent if manual arming occurs before the closing time period begins. Missed Opening/Closing type reports are programmed in the Report Code Programming. The Exception Reporting option must be set for these to be sent.		<div>Closing Window</div> <p>No reports are sent if system is armed* during this time period.</p> <p>* or disarmed if user needs to re-enter premises.</p>		Auto-arm delay begins. Auto-arm warning begins. Auto-arm occurs after warning expires (if auto-arm is enabled). Missed Closing reports are sent if manual arming has not occurred at expiration of closing time period. Late Closing reports are sent if system is manually armed after the closing time period expires.	

Scheduling Menu Mode

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

The following can be programmed while in this mode:

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

Some scheduling features are programmed in Data Field Programming Mode (**Installer Code + 8 0 0 0**).

Some features are programmed in the #93 Menu Mode located in the Programming Guide.

The general programming scheduling fields are listed below.

System-Wide Fields:	
*04	Enable Random Timers
1*74 –1*75	Relay timeout values
2*01-2*02	Summer Time options
2*11	Allow disarming outside time period 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 time periods
#93 Menu Mode (System Group #3)	
Scheduling related report codes	

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

Steps to Program Scheduling Options

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

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

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

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

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

Scheduling Menu Structure

To program schedules, enter Scheduling Program Mode enter the **Installer Code + [#] + [80]**. (Installer or Master level user code.)



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

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

PROMPT	EXPLANATION
Time Window ? 1 = YES 0 = NO 0	Upon entering Schedule Menu Mode, this prompt appears. Enter 1 to program time periods. Refer to <i>Time Periods Programming</i> later in this section for detailed procedures. Enter 0 to move to the "O/C Schedules?" prompt.
O/C Schedules ? 1 = YES 0 = NO 0	Enter 1 to program opening and closing schedules. Refer to <i>Open/Close Schedules Programming</i> later in this section for detailed procedures. Enter 0 to move to the "Holidays?" prompt.
Holidays ? 1 = YES 0 = NO 0	Enter 1 to program holiday schedules. Refer to <i>Holiday Schedule Programming</i> later in this section for detailed procedures. Enter 0 to move to the "Timed Events?" prompt.
Timed Events ? 1 = YES 0 = NO 0	Enter 1 to program timed events for relay outputs, additional schedules, and other system functions. Refer to <i>Time-Driven Event Programming</i> later in this section for detailed procedures. Enter 0 to move to the "Access Sched?" prompt.

PROMPT	EXPLANATION
--------	-------------

Access Sched. ?
1 = YES 0 = NO 0

Enter **1** to program access schedules. Refer to *Limitation of Access Schedules Programming* later in this section for detailed procedures.
Enter **0** to move to the "Quit?" prompt.

Quit ?
1 = YES 0 = NO 0

Enter **1** to quit **#80 Scheduling Menu Mode** and return to normal operating mode.
Enter **0** to make any changes or review the scheduling programming options. If you press **0**, the "Time Window?" prompt is displayed.

Time Periods

Twenty (20) time periods are provided for use in open/close and access schedules, as well as for output controls, and are the basis of the scheduling system. These time periods are shared among all 8 partitions. A time period must have a start and a stop time.

Time Periods Worksheet

The following worksheet is an example of the worksheet found in the *Programming Guide*. This worksheet will help you define time periods and scheduling aspects of this system before you program them. Note that time periods **can** span midnight; for example, from 2300 to 0100.

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

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

Time Periods Programming

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

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



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

Daily Open/Close Schedules

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

Open/Close Schedule Worksheet

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

Part	Mon	Tues	Wed	Thur	Fri	Sat	Sun	Hol
------	-----	------	-----	------	-----	-----	-----	-----

	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl	Op	Cl
1																
2																
3...8																

Open/Close Schedule Programming

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

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

Holiday Schedules

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

Holiday Schedule Worksheet

Use the following worksheet to record the 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 below. 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.

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

Time Driven Events

These 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 periods.

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

Time-Driven Events Worksheet

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

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

1. Enter the schedule number (01-20) and time period number (01-20), and note the day of the week the action is desired.

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

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

Relay Commands

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

Arm/Disarm Commands

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



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

Bypass Commands

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

Open/Close Time Periods

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

Access Control Commands

Action Code	Action	Action Specifier
55	Access Point Grant	Access Point #
56	Access Point Grant with Override	Access Point #
57	Access Point Protect	Access Point #
58	Access Point Bypass	Access Point #
59	Access Point Lock	Access Point #
60	Access Point Exit	Access Point #
61	Access Point Group Grant	Group #
62	Access Point Group Grant with Override	Group #
63	Access Point Group Protect	Group #
64	Access Point Group Bypass	Group #
65	Access Point Group Lock	Group #
66	Access Point Group Exit	Group #
67	Access Point Partition Grant	Partition #
68	Access Point Partition Grant with Override	Partition #
69	Access Point Protect by Partition	Partition #
70	Access Point Bypass by Partition	Partition #
71	Access Point Lock by Partition	Partition #
72	Access Point Exit by Partition	Partition #
73	Access Point Trigger On	Trigger #
74	Access Point Trigger Off	Trigger #
77	Access Point Group Enable	Group #
78	Access Point Group Disable	Group #

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

Activation Time	Description
01	Beginning of time period.
02	End of time period.
03	During time period only (on at beginning of time period, off at end). For example, if bypass is selected to activate during the time period, zones in a zone list are bypassed at the beginning of the time period and unbypassed at the end of the time period.
04	Beginning and end of time period (e.g., a coffee break buzzer). In this example, if relay pulse is selected, the relay pulses for 2 seconds at the beginning of the time period, signaling the beginning of the coffee break. At the end of the time period it pulses again, signaling the end of coffee break.

Time-Driven Event Programming

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

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

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

PROMPT	EXPLANATION	
<div>Timed Events ? 1 = YES 0 = NO 0</div>	Enter 1 to program timed events.	
<div>TIMED EVENT # ? 01-20, 00=Quit 01</div>	Enter the timed event number to be programmed (01-20). Press [*]. The system then prompts the user to enter the desired action to be taken. Enter 00 at the "TIMED EVENT #?" prompt to quit the timed event menus and display the "Quit ?" prompt.	
<div>01 ACTION ? none 00</div>	Enter the action code for this timed-event number from the list at the left. This could be an output command, an arming command, or any other Time-Driven event. Press [*] to accept the entry. The prompt for the action specifier appears.	
ACTION CODES	EXPLANATION	ACTION SPECIFIER
01=Relay On 02=Relay Off 03=Relay Close for 2 seconds 04=Relay Close XX minutes 05=Relay Close YY seconds	Actions 01-05 If you selected actions 01-05 , the prompt at the right appears. Enter the relay number. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 RELAY # ? 00</div>
06=Relay Group On 07=Relay Group Off 08=Relay Group Close for 2 seconds 09=Relay Group Close XX minutes 10=Relay Group Close YY seconds	Actions 06-10 If you selected actions 06-10 , the prompt at the right appears. Enter the relay group number. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 RELAY GRP # ? 00</div>
20=Arm-STAY 21=Arm AWAY 22=Disarm 23=Force Arm STAY 24=Force Arm AWAY 25=Arm INSTANT 26=Arm MAXIMUM 40=Enable Open Time Period by Part. 41=Enable Close Time Period by Part.	Actions 21-26 and 40-41 If you selected actions 21-26 or 40-41 , the prompt at the right appears. Enter the partition to which the action applies. Enter 0 to select all partitions. Enter a partition number again to deselect it. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>PART? 12345678 HIT 0-8 X X</div>
30=Auto bypass – Zone list 31=Auto unbypass – Zone list	Actions 30-31 If you selected actions 30-31 , the prompt at the right appears. Enter the zone list number that contains the zones to be bypassed or unbypassed. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 ZONE LIST ? ENTER 01-15 01</div>

ACTION CODES	EXPLANATION	ACTION SPECIFIER
42=Enable Access Time Period for Access group(s)	Action 42 If you selected action 42 , the prompt at the right appears. Enter the group number to which the time period will apply. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>GROUP ? 12345678</div> <div>HIT 0-8 X</div>
55=Access Point Grant 56=Access Point Grant w/Override 57=Access Point Protect 58=Access Point Bypass 59=Access Point Lock 60=Access Point Exit	Actions 55-60 If you selected actions 55-60 , the prompt at the right appears. Enter the access point number. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 ACCESS POINT #</div> <div>000</div>
61=Access Point Group Grant 62=Access Point Group Grant w/Override 63=Access Point Group Protect 64=Access Point Group Bypass 65=Access Point Group Lock 66=Access Point Group Exit 77=Access Point Group Enable 78=Access Point Group Disable	Actions 61-66 and 77-78 If you selected actions 61-66 , the prompt at the right appears. Enter the group number. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 GROUP #</div> <div>00</div>
67=Access Point Partition Grant 68=Access Point Partition Grant w/Override 69=Access Point Protect by Partition 70=Access Point Bypass by Partition 71=Access Point Lock by Partition 72=Access Point Exit by Partition	Actions 67-72 If you selected actions 67-72 , the prompt at the right appears. Enter the partition to which the action applies. Enter 0 to select all partitions. Enter a partition number again to deselect it. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>PART? 12345678</div> <div>HIT 0-8 X X</div>
73=Access Point Trigger On 74=Access Point Trigger Off	Actions 73-74 If actions 73-74 were selected, the prompt at the right will be displayed. Enter the trigger number. Press [*] to accept entry. The "Time Window ?" prompt appears.	<div>01 TRIGGER #</div> <div>00</div>
PROMPT	EXPLANATION	
<div>01 Time Window ?</div> <div>00:00 00:00 01</div>	Enter the time period 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 period number is displayed. Press [*] to accept entry.	
<div>01 Active time ?</div> <div>00</div>	Enter the activation time from 1-10 (listed below). As the number is keyed in, the activation time is displayed. The choices are: 01: Trigger at the start of the time period. 02: Trigger at the end of the time period. 03: Take effect only for the duration of the time period. 04: Trigger at both the start and the end of the time period. Example: coffee break buzzer. Press [*] to accept entry.	
<div>Days ? MTWTFSSH</div> <div>Hit 0-8 x x</div>	The system then asks for which days the event is to be activated. Press 0 to toggle all days on or off; or press keys 1-8 to toggle the letter "x" under the day on or off (Monday = 1, Holiday = H = 8). When all entries have been made, the "TIMED EVENT #?" prompt is displayed again. Repeat the procedure for each timed event for the installation.	

PROMPT	EXPLANATION
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 periods for each day of the week and two time periods for holidays (typically, one for an opening time period and the second for a closing time period).

A user, required to follow a schedule, would be assigned to an access group of the same number (e.g., schedule 1= group 1).

The user's access code is assigned to a group when that user is added to the system. If no limitations apply, enter **0**.

NOTE: Holidays used for access groups are those defined for partition 1 only.

Limitation of Access Schedule Worksheet

Enter the appropriate time period numbers for each access schedule.

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

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.

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

PROMPT	EXPLANATION
<div>Quit ?</div> <div>1 = YES 0 = NO 0</div>	Enter 0 at the "Quit ?" prompt to return to the main menu choices and continue programming. Enter 1 to quit Scheduling Menu Mode.

Temporary Schedules

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

Only users with the authority level of manager or higher can program temporary schedules. A temporary schedule affects only the partition from which it is entered. Temporary schedules can also be reused at later dates simply by scrolling (pressing [#]) to the "DAYS?" prompt and activating the appropriate days. This should be considered when defining daily time periods.

Temporary Schedule Worksheet

Partition/Time Periods		Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	Disarm Time Period							
	Start Time HH:MM							
	Stop Time HH:MM							
	Arm Time Period							
	Start Time HH:MM							
	Stop Time HH:MM							
2...8	Disarm Time Period							
	Start Time HH:MM							
	Stop Time HH:MM							
	Arm Time Period							
	Start Time HH:MM							
	Stop Time HH:MM							

Temporary Schedules Programming

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

PROMPT	EXPLANATION
<div>Mon DISARM WIND.</div> <div>00:00 00:00</div>	This prompt is for entering the start and end times of the disarm (opening) time period for Monday. Upon entry of this mode, the cursor is positioned on the tens of hours digit of the start time of the disarm time period. Enter the desired hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. Repeat the procedure for the stop time entry. Press [*] to store the entries and move to the arming (closing) time period for Monday. Pressing [#] scrolls you through the prompts without making any changes.
<div>Mon ARM WINDOW</div> <div>00:00 00:00</div>	This prompt is for entering the start and end times of the arm (closing) time period for Monday. The cursor is positioned on the tens of hours digit of the start time of the arm time period. Enter the desired hour. Press [*] to move to the minutes field. The minutes are entered in the same manner. Repeat the procedure for the stop time entry. After the time periods for that day have been completed, the system prompts for disarm and arm time periods for the next day. Press [#] if no changes are desired.
<div>Tue DISARM WIND.</div> <div>00:00 00:00</div>	Repeat the procedure described above for all days of the week. When all the time periods for all the days have been completed, the system prompts for which days of the schedule are to be activated.

PROMPT	EXPLANATION
<div>Days ? MTWTFSS</div> <div>Hit 0-7 x x</div>	<p>This is the prompt that actually activates the temporary schedule.</p> <p>To select the days to be activated, enter 1-7 (Monday = 1). An "X" appears under that day, indicating the temporary schedule for that day is active. Entering a day's number again deactivates that day. Pressing 0 toggles all days on/off.</p> <p>The temporary schedule is in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, but all other entries for the temporary schedule remain programmed.</p> <p>Press [*] to store the entries or press [#] to exit the Temporary Schedule Entry Mode without making any changes.</p>

User Scheduling Menu Mode

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

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

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

PROMPT	EXPLANATION
<div>Output Timer # ?</div> <div>01-20, 00=Quit 01</div>	<p>Enter the output timer number to be programmed (01-20).</p> <p>Press [*] to accept entry and move to the next prompt.</p> <p>Enter 00 to quit and return to normal operating mode.</p>
<div>06 19:00 23:45</div> <div>PORCH LITE 04</div>	<p>If that timer number has already been programmed, a summary screen appears. In this example:</p> <p>06 = Timer #</p> <p>07:00PM = Start Time</p> <p>11:45PM = Stop Time</p> <p>PORCH LITE = Descriptor for Output Device # 4</p> <p>04 = Output Device # affected by this timer</p> <p>Press [*] to continue.</p>
<div>06 ENTER OUTPUT#</div> <div>PORCH LITE 04</div>	<p>Enter the desired output number (01-96).</p> <p>As the number is entered, the descriptor for that output device is displayed.</p> <p>Press [*] to continue.</p>



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

PROMPT	EXPLANATION
<div>06 ON TIME ?</div> <div>19:00</div>	<p>The cursor is positioned on the tens of hours digit of the ON time. Enter the desired hour.</p> <p>Press [*] to move to the minutes field. The minutes are entered in the same manner.</p> <p>Press [*] to continue.</p>
<div>06 OFF TIME ?</div> <div>23:45</div>	<p>The cursor positioned on the tens of hours digit of the OFF time. Enter the desired hour.</p> <p>Press [*] to move to the minutes field. The minutes are entered in the same manner.</p> <p>Press [*] to continue.</p>
<div>06 DAYS? MTWTFSS</div> <div>HIT 0-7 x x</div>	<p>To select the days to be activated, enter 1-7 (Monday = 1). An "x" appears under that day, indicating the output for that day is active. Entering a day's number again deactivates that day. Pressing 0 toggles all days on/off.</p> <p>The outputs are in effect only for the days highlighted with the letter "x" under them. As the week progresses, the selected days are reset to the inactive state, unless the permanent option is selected (next screen prompt).</p> <p>When completed, press [*] to continue.</p>

PROMPT	EXPLANATION
06 Permanent ? 0 = NO,1 = YES 0	Selecting "Permanent" (1) means that this schedule will be in effect on a continuous basis. Selecting 0 means that this schedule will be in effect for one week only. The letter "x" under the day is then cleared, but all other entries for the output device remain programmed. Press [*] to accept entry. The system quits User Scheduling Mode and returns to normal operating mode.

Downloading

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 Pentium computer with at least 16MB RAM, a hard disk with 40MB available disk space, CD ROM drive, a display with 800 x 600 pixel resolution, running Windows 95, 98 (2nd edition), or Windows NT.
2. An ADEMCO designated compatible modem, such as CIA, CIA-EU, CIA-AU from ADEMCO.
3. Alternately, you may use a 4100SM interface module to "direct wire" the control panel to your computer at the site.
4. COMPASS DOWNLOADING software, from ADEMCO. This software is available on CD ROM and includes a complete User's Manual.

Getting On-Line with a Control Panel

At the protected premises, the Control panel must be connected to the existing telephone line (refer to **SECTION 3: Installing the Control**). No programming of the panel is required before downloading to an initial installation. In order to remotely access, control, or program the alarm panel, a "link" must be established between the computer and the control panel.

To download to a panel that is not programmed, do the following:

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.
3. The downloader will establish a session with no callback. The panel information can then be downloaded.

To download to a panel that is already programmed, do the following:

1. The computer calls up the Control panel. (The phone number for each customer is entered into the customer's account file on the computer).
2. The Control panel "answers" at the pre-programmed ring count and executes a handshake with the computer.
3. The computer sends a request for call-back to the Control, unless call-back is not required.
4. 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 data in its own memory.
5. Upon a successful match, the Control panel will seize the phone line and call the computer back, unless call-back is not required.
6. The computer answers, usually by the second ring, and executes a handshake with the panel.
7. The panel then sends other default information to the computer. If this information matches the computer's information, a successful link is established. This is known as being "ON-LINE".



Alarm and trouble responses are disabled during EEROM update while on-line. Should an event occur during this time, the response and the report will go through as soon as the remote access sequence is completed. At other times during the on-line session, the control signals the PC and breaks off the session to transmit alarms. The keypads are inactive during downloading communication.

Downloading Notes

- Each time the Control panel is accessed successfully, a Program Tamper report (*81) is sent to central station, if programmed.
- When downloading, the keypad displays "MODEM COMM."
- Whenever a download or a save is done, an automatic time stamp is done, indicating the date and time of the last download (or save) and the operator ID number.
- The average time for a complete download, including initial call-up, hang-up and call-back is under 4 minutes.
- 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 distributor for printer recommendations.

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 (if field *38 Armed Restriction is not programmed)
- Bypass a Zone
- Force the System to Accept a New Program Download
- Shut Down Communication (dialler) 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 Mains Status, List of Faulted Zones, List of Bypassed Zones, 512 Event Log, List of Zones Currently in Alarm, List of Zones Currently in Trouble
- Set the Real-Time clock.
- Initiate a test report from the control.
- Command relays/triggers to activate and de-activate.

Access Security

Accessing the Control from a remote location is protected against compromise by the use of 4 levels of protection:

- **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.
- **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.
- **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. Additionally, all account files are encrypted to prevent them from being opened on another installer's COMPASS downloading software package.
- **Operator Access Levels:** Up to 15 operators can have access to the DOWNLOADER, each having their own log-on code. However, each operator can be assigned one of three levels of access in both FILE and COMMAND functions, as follows:

File Access

Read Only: able only to look at the database; cannot change any information, and cannot see the customer's access codes.

Part Read/Write: able to look at and change all information, except the customer's access codes.

Full Read/Write: able to look at and change any and all information in the database.

Control/Comm Access

Read Only: able only to Upload and arm the system. Not able to DISARM, BYPASS, or change any information.

Part Read/Write: able to ARM, BYPASS, UPLOAD, DOWNLOAD but cannot shutdown the system.

Full Read/Write: able to perform all control and status commands, as well as shutdown all or part of the system.

Connecting a 4100SM Module for Direct Wire Downloading

The Control can be downloaded without using a modem or telephone line by using COMPASS Software and a 4100SM Serial Module. 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 *Figure 7-1* for the correct connections. In addition, when the "green" wire is referred to in step 2 of the IN CASE OF DIFFICULTY section of the 4100SM Instructions, use the "violet" wire.

Connector J8, located above connector J7 on the right hand side of 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 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.**

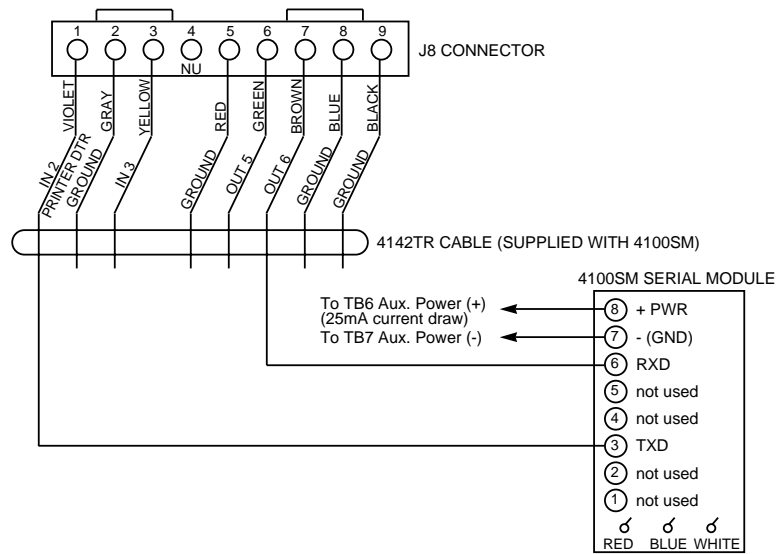


Figure 7-1. Direct Wire Downloading Connections

Setting The Real-Time Clock

General Information

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



Use an 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

1. Enter installer or master code + # 63. Typical display shows

TIME/DATE	—	THU
12:01		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, day, month, and year.
 Press the * key to accept the entered value. The cursor then moves to the right.
 Press the # key to move the cursor to the left of the display, to the previous position.
 Enter the correct hour then press * to move to the minutes and make the correct entry.
 Press * to move cursor to the day position and enter the correct day using a 2-digit entry.
 Press * and enter the correct month.
 Press * and enter the correct year.
3. Exit clock mode by pressing the * key after the cursor is in the year position.



Be sure to select the correct sync source for the Real-Time Clock (AC or the internal crystal) in field 1 * 54. If you select the internal crystal, use fields 1 * 50 and 1 * 51 to compensate for any internal crystal inaccuracies.

Security Access Codes

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 given access to only some partitions, its user ID number cannot be used again for a different code in the other partitions.**

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



User #2 must be programmed for the Quick Arm feature to function.

In order to protect the system from attempts to defeat the security access code by trying many possible codes in sequence, the system has code tampering protection. If someone enters 20 keystrokes at a keypad within a 15 minute time period, all further keypad entries from keypads in this partition will be ignored for the 15 minute time period. This protection will then be repeated indefinitely.

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.

Use the “View Capabilities” keypad function (**User Code + [*] + [*]**) to view the partitions and authority levels for which a particular user is authorized. These levels are described in the following table in order from highest to lowest ranking.

Level 0: Installer (User 1) Code

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

Level 1: Master Codes

- Can perform all normal system functions.
- Can be used to assign up to 148 lower-level codes, which can be used by other users of the system.
- Cannot assign anybody a level of 0 or 1.
- May change 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 is automatically the **same** as that of the Master who is adding the new user.

Level 2: Manager Codes

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

Levels 3-5: Operator Codes

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

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

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

Level 6: Duress Codes

- Sends a silent alarm to a central monitoring station if the user is being forced to disarm (or arm) the system under threat (system must be connected to a central station).
- When the system's Auxiliary Voltage Triggers are connected to another communication's media (Derived Channel/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.

General Rules on Authority Levels and Changes

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

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



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

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

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

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



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

Multiple Partition Access

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

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

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

EXAMPLE OF MULTIPLE PARTITION ACCESS

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

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

Adding a Master, Manager, or Operator Code



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

Enter **Installer Code[†] + [8] + new user no. (002-150) + new user's code**

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

PROMPT	EXPLANATION
User Number = 003 Enter Auth. Level	Enter the level number as follows: 1 = Master 4 = Operator Level B 2 = Manager 5 = Operator Level C 3 = Operator Level A 6 = Duress Keypad then prompts for Open/Close reporting option for this user.
Open/Close Rep.? 0 = NO , 1 = YES	Press 0 (NO) or 1 (YES), depending on whether or not arming/disarming by this user will trigger Opening and Closing reports. This prompt appears only if the Installer Code is used to add a user.
Access Group? Enter 0-8	If access schedules have been programmed, this prompt appears. Enter the user's access group number (1-8) if this user should have limited access to the system. Enter 0 if no access group should be assigned.
RF Button ? 0=NO , 1=YES	If a 5800 Series button transmitter has been enabled for arming/disarming functions, and is not assigned to a user, this prompt appears. Press 0 (NO) or 1 (YES).
Enter Button ZN # (001-087)	If you answered "yes" to the RF button question, the zone number for the button is requested. Enter any one of the zone numbers assigned to the button transmitter as AWAY, STAY, or DISARM. The system then assigns all buttons of the transmitter to this user number.
Multi-Access ? 0 = NO , 1 = YES	Press 0 (NO) if the user is to have access to this partition only. Press 1 (YES) if the user is to have access to more than one partition. If NO, the program exits this mode. If YES, the keypad prompts for the Global Arm option for this user.
Global Arm ? 0 = NO , 1 = YES	Press 0 (NO) or 1 (YES), depending on whether this user will be allowed to arm more than one partition via Global Arm prompts (described in <i>SECTION 11: Keypad Functions</i>). The keypad now prompts for the user's access to the next partition.
Part. 2 – SHOP ? 0 = NO , 1 = YES	Press 0 (NO) or 1 (YES), depending on whether this user will have access to the displayed partition number. If NO, the keypad displays this prompt for the next partition number in sequence. If YES, the keypad prompts for the following: <ul style="list-style-type: none"> • User's authority level in the displayed partition (see Authority Level prompt above). • Open/Close option for this user in the displayed partition (see Open/Close prompt above). • Global Arm option for this user in the displayed partition. When all partitions have been displayed, the keypad will scroll through all partitions to which access has been assigned, and will display the user number, authority level, open/close and global arm options that were programmed for each partition to which the user was granted access. For example:
Part. 1 A0T WHSE User 003 Auth=3G.	Note that the "G" following the authority level indicates that the global arm feature is enabled for this user in the displayed partition, and that the time period at the end of the second line indicates Open/Close reporting is enabled for this user in the displayed partition. The "T" indicates the partition from which the user may be changed or deleted.

Changing a Master, Manager, or Operator Code

Enter **Installer Code*** + [8] + **new user no. (002-150)** + **new user's code**

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

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

Adding an RF Key to an Existing User

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

Deleting a Master, Manager, or Operator Code

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

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

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



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

Exiting the User Edit Mode

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

Testing The System

Battery Test

When AC power is present, the VISTA-120IT runs a brief (13 seconds) battery test every 4 minutes (alternately, the test can be for 1.5 seconds every 50 seconds) to determine if there is a battery connected, and runs an extended battery test every 24 hours to check on the battery's condition. This presence test is conducted whenever the system or a partition is disarmed.

If the VISTA-120IT finds that the battery voltage is low (less than approximately 11.5V, 10.8 in the VISTA-120FR), it initiates a keypad "SYSTEM LOBAT" display and a rapid keypad beeping sound. It also sends a Low Battery report to the central station (if programmed). The keypad is cleared by entering any security code + OFF, and a Restore report is sent to the central station if the situation has been corrected.

Dialler Test

The VISTA-120IT 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).

The system can be programmed to send the first report at any time of the day, or on any day of the week (field *83).

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



Whenever the Test Mode is entered from a keypad, the system performs a LCD Display Test. This activates all LEDs and LCD dots (that make up characters) for 2-3 seconds. If the system includes Quest 2260SN PIRs, see Testing the Quest 2260SN for specific testing instructions.

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. Note that while this test is active the system will not trigger alarms for burglary and non-fire related 24-hour zones, but will trigger fire alarms. This test can be activated only by the Installer, Master or Manager-level users, by entering the corresponding security code and pressing TEST while the burglary portion of the system is disarmed.

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

Open and close each protected door and window in turn. Each action should produce 3 beeps from the keypad. Walk in front of any motion detectors. Listen for three beeps when the detector senses movement. The keypad displays the zone number and alpha descriptor while a door or window remains open or while a detector remains activated. 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 is sent to the central station.

Testing the Quest 2260SN

Normally, in the test mode, the LED on the Quest 2260SN PIR is disabled. In order to have the LED illuminate during the test mode, the PIR zone number must be entered into the system's test memory. To do this, enter [zone number] + [#]. To remove a zone from the system's test memory, enter [zone number] + [*].

NOTES:

1 beep indicates a correct zone number entry.

2 beeps indicate an incorrect entry.

The system's test memory capacity is 5 zones.

When the test mode is exited the system's test memory is cleared.

Armed Burglary System Test



Alarm messages are 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, proceed as follows:

1. Notify the central station that a test of the system is being performed.
2. Arm the system.
3. Fault one or more zones.

Silence alarm sounder(s) each time by entering the code and pressing OFF.

NOTE: The system must be rearmed after each code + off sequence.

Check that entry/exit delay zones provide the assigned delay times.

Check the keypad-initiated alarms, if programmed, by pressing the panic key pairs (* and #, 1 and *, and/or 3 and #).

The word ALARM and a descriptor "999" are displayed for * and #. If [1] and [*] are pressed, "995" is displayed; if [3] and [#] are pressed, "996" is displayed.

If the system has been programmed for audible emergency, the keypad emits a loud, steady alarm sound. Silence the alarm by entering the security code and pressing OFF. If the system has been programmed for silent panic, there are no audible alarms or displays. A report is sent to the central station, however.

Notify the central station that all tests are finished, and verify results with them.

Testing Wireless Transmitters

Transmitter ID Sniffer Mode

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



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

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

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

Go/No Go Test Mode

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



All partitions containing wireless transmitters must be placed in the test mode for sensitivity reduction of the RF receiver (50% sensitivity). Otherwise, the RF receiver remains at full strength.

Make sure that all partitions are disarmed when performing this test, as the wireless receiver gain is reduced in half.

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

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

Trouble Conditions

Check or Trouble Messages

Display	Description
CHECK or TRBL (as per field 1*07)	This indicates that a problem exists on the zone number displayed. Zone trouble may be caused by one of the following conditions: <ul style="list-style-type: none"> • A wired fire zone is open (broken wire). • A Day/Night zone (zone type 5) is faulted. • A polling loop zone is not seen by the control panel. • A polling loop zone has been tampered (cover removed on a 4190). • A wireless zone has not checked in during the time programmed in field 1*31. • A 5800 Series transmitter has been tampered (cover removed).
CHECK 8XX XX = 00-30	This indicates a trouble on a peripheral device (connected to the panel's keypad terminals) of the corresponding device address (00-30).
CHECK 9XX XX = 00-99	This indicates that a system trouble exists (RF receiver, bell output, etc.). See <i>SECTION 4: Programming</i> .



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

Other System Messages

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

Power Failure

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

Telephone Operational Problems

In the event of telephone operational problems, disconnect the control panel by removing the plug from the RJ31X 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.

To the Installer

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

The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts.

Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Turning the System over to the User

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

Specifications

VISTA-120IT CONTROL

Physical:	318mm Wide X 368mm High X 76mm Deep
Electrical:	
Voltage Input:	In 110 volt AC mains systems, from ADEMCO No. 1361 Plug-In Transformer or 4300 transformer (for X-10 installations) rated 16.5VAC, 40 VA or XF10 transformer (for 220VAC, 50Hz X-10 installations)
Alarm Sounder Output:	10VDC-13.8VDC (10.7VAC-14.5VAC for VISTA-120FR), 2.8 amps max.; 750mA less aux. current drain
Auxiliary Power Output:	9.6VDC-13.8VDC, 750mA max.
Backup Battery:	12VDC, 4AH or 7AH gel cell. No. 467 (12V, 4AH) or 712BNP (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, Robofon Contact ID, ADEMCO Contact ID, SESCOA and Radionics Low Speed
Line Seize:	Double Pole

Remote Keypads

6139

Physical:	
Width:	150mm
Height:	121mm
Depth:	32mm
Electrical:	
Voltage Input:	12VDC
Current Drain:	100mA
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

6164

Physical:	
Width:	187mm
Height:	137mm
Depth:	32mm
Electrical:	
Voltage Input:	12VDC
Current Drain:	55-190mA
Interface Wiring:	
RED:	12VDC input (+) auxiliary power
BLACK:	Ground and (-) connection from supplemental power supply
GREEN:	Data to control panel
YELLOW:	Data from control panel

The following terminals on the 6164 are not used with the VISTA-120IT:

Z1
↓
Z2
Z3
↓
Z4
NO
C
NC
↓

Contact ID and Event Log Codes

Table of Contact ID Event Codes

Code	Definition	Code	Definition
110	Fire Alarm	389	Detector Self-Test Failed
111	Smoke Alarm (Fire w/Verification)	401	O/C By User
113	Water Flow Alarm	403	Power-Up Armed/Auto-Arm
121	Duress	406	Cancel by User
122	Silent Panic	407	Remote Arm/Disarm (Download)
123	Audible Panic	408	Quick Arm
124	Duress Access Grant	409	Keyswitch O/C
125	Duress Egress Grant	411	Call back Requested
131	Perimetre Burglary	421	Access Denied
132	Interior Burglary	422	Access Granted
133	24 Hour Burglary	423	Door Force Open
134	Entry/Exit Burglary	424	Egress Denied
135	Day/Night Burglary	425	Egress Granted
140	ACS Zone Alarm	426	Door Prop Open
142	Polling Loop Short Alarm	427	Access Point DSM Trouble
150	24 Hour Auxiliary	428	Access Point RTE Trouble
200	Fire Supervisory	429	ACS Program Entry
301	AC Loss	430	ACS Program Exit
302	Low System Battery	431	ACS Threat Change
305	System Reset	432	Access Point Relay/Trigger Fail
306	Program Tamper	433	Access Point RTE Shunt
308	System Shutdown	434	Access Point DSM Shunt/Unshunt
309	Battery Test Fail	441	Armed STAY
310	Ground Fault	451	Early Open/Close
313	System Engineer Reset	452	Late Open/Close
320	ACS Relay Supervision	453	Fail to Open
321	Bell Trouble	454	Fail to Close
332	Poll Loop Short-Trouble	455	Auto-arm Fail
333	Expansion Module Failure	457	Exit Error by User
338	ACS Module Low Battery	459	Recent Close
339	ACS Module Reset	501	ACS Reader Disable
342	ACS Module AC Loss	520	ACS Relay Disable
343	ACS Module Self-Test Fail	521	Bell 1 Bypass
351	Main Dialler Trouble	522	Bell 2 Bypass
352	Backup Dialler Trouble	524	Auxiliary Relay Bypass
354	ACS RS232 Fail	551	Main/Backup Dialler Bypass
373	Fire Loop Trouble	570	Bypass
374	Exit Error by Zone	576	ACS Zone Shunt
380	Trouble (global)	577	ACS Point Bypass
381	Loss of Supervision (RF)	602	Communicator Test
382	Loss of RPM Supervision	604	Fire Test
383	RPM Sensor Tamper	607	Burglary Walk Test
384	RF Transmitter Low Battery	608	Off-Normal
385	High Sensitivity Maintenance Signal	611	Fire Walk Test – Point Tested
386	Low Sensitivity Maintenance Signal	612	Fire Walk Test – Point Not Tested

Code	Definition	Code	Definition
621	Event Log Reset	625	Time/Date Reset
622	Event Log 50% Full	631	Exception Schedule Change
623	Event Log 90% Full	632	Access Schedule Change
624	Event Log Overflow		

Table of Event Log Codes

Event	Alpha	Event	Alpha
Access Control Test Mode Start	BGN ACS TEST	Door Forced Open	DR FORCE
Access Control Test Mode End	END ACS TEST	Door Forced Open Restore	DRFO RST
Access Denied	NO ENTRY	Door Prop Open	DR OPEN
Access Granted	ENTERED	Door Prop Open Restore	DRPO RST
Access Point Bypass	ACPT BYP	Duress Access Grant	DUR ACCS
Access Point DSM Shunt	DSM SHNT	Duress Alarm	DURESS
Access Point DSM Trouble	DSM TRBL	Duress Egress Grant	DUR EXIT
Access Point DSM Trouble Restore	DSM RST	Duress Restore	DURE RST
Access Point Failure	ACS PNT	Egress Denied	NO EXIT
Access Point Failure Restore	ACPT RST	Egress Granted	EXITED
Access Point Relay Supervision Fail	ACPT RLY	Entry to Test Mode	TEST ENTRY
Access Point Relay Supervision Restore	RLY RST	Event Log	LOG OVERFLOW
Access Point RTE Shunt	RTE SHUNT	Event Log Cleared	LOG CLEARED
Access Point RTE Trouble	RTE TRBL	Event Log at 50% Capacity	LOG 50% FULL
Access Point RTE Trouble Restore	RTE RST	Event Log at 90% Capacity	LOG 90% FULL
Access Point Unbypass	ACPT UNB	Exit Error Occurred	EXIT ERR
Access Point DSM Unshunt	DSM UNSH	Exit From Program Mode	PROGRAM EXIT
Access Point RTE Unshunt	RTE UNSH	Exit From Test Mode	TEST EXIT
AC Loss at a Module	ACLO MOD	Failure to Communicate	FAIL TO COMM
AC Loss at a Module Restore	ACRST MOD	Fire Alarm	FIRE
AC Power Fail	AC LOSS	Fire Alarm Restore	FIRE RST
AC Power Restore	AC RESTORE	Fire Zone Trouble	FIRE TRB
ACS Module Reset	RES MOD	Fire Zone Trouble Restore	FRTR RST
ACS Program Entry	ACS PROG	Intrusion Verify	INTRSN VERIF
ACS Program Exit	ACS PRGX	Low Battery at a Module	LBAT MOD
ACS Reader Disable	RDR DISA	Low Battery at a Module Restore	LBAT RST
ACS Reader Enable	RDR ENAB	Non-Burglar Alarm	AUXILARY
ACS Relay/Trigger Disable	RLY DISA	Non-Burglar Restart	AUX RST
ACS Relay/Trigger Enable	RLY ENAB	Override AC Loss/Comm Fail/Sys Low Bat	OVERRIDE TRBU
ACS Threat Change	THRT CHG	Panel is Calling Download Computer	CALL BACK
ACS Zone Alarm	ZN ALARM	Panic Alarm	PANIC
ACS Zone Alarm Restore	ZNAL RST	Panic Alarm Restore	PNC RST
ACS Zone Change	ACZN CHG	Poll Loop Restore	EXP RST
ACS Zone Shunt	ZN SHUNT	Polling Loop RPM Restore	RPM RST
ACS Zone Unshunt	ZN UNSHT	Poll Loop Short	EXP SHRT
Auto Disarm	DISARM-AUTO	Poll Loop Smoke Det. Tested†	TESTED
Backup Battery Test Failed	BAT TST FAIL	Poll Loop Smoke Det. Not Tested†	UNTESTED
Burglary Alarm	BURGLARY	Poll Loop Smoke Det. Test Failed†	FAILED
Burglary Alarm Cancel	CANCEL	Polling Loop Short	EXP TRBL
Burglary Alarm Restore	BURG RST	Polling Loop Tamper	EXP TMPR
Comm. Failure from MLB to Module	COMM MOD	Printer Failure	PRINTER FAIL
Comm. from MLB to Module Rest	COMM RST	Printer Restore	PRINTER RST
Communication Restore	COMM RESTORE	Programmed Access Sched Change	ACC SKED CHG
Dialler Restored to Service	DIALLER RST	Program Change	PROG CHANGE
Dialler Shutdown	DIALLER SHUT	Program Mode Entered	PROGRAM ENTRY
Disarmed	DISARMED	Programmed Schedule was Changed	SCHEDULE CHANGE

Event	Alpha	Event	Alpha
Real-Time Clock was Set	TIME SET	System Did Not Disarm by Schedule	MISSED DISRM
RF Expander Module Fail	RF EXPND	System Disarmed Remotely	DISARMED-REM
RF Expander Module Restart	RF RST	System Disarmed by RF Key	DISARMED-KEY
RF Receiver Trouble	RF TRBL	System Disarmed Earlier than Sched	DISRMD-EARLY
RF Receiver Trouble Restore	RF RST	System Disarmed Later than Sched	DISRMD-LATE
RF Transmitter Low Battery	RF LBAT	System Engineer Reset	SYS RST
RF Transmitter Low Battery Restore	RFLB RST	System Low battery	LOW BATTERY
RF Transmitter Low Battery Test	RF LB OK	System Shutdown	SYS SHUT
RF Transmitter/Rcvr Supvs Fail	RF SUPR	Sys Batt Fail or Disconnection	BATTERY FAIL
RF Transmitter/Rcvr Supvs/Tble Rest.	RF RST	System Shutdown Restore	SYSSHTRST
Scheduled System Arming Failed	ARM FAILED	Supervised Relay Trouble	RLY TRBL
Self Test Failed at a Module	SELF MOD	Supervised Relay Restore	RLY RST
Self Test at a Module Restore	SELF RST	System Restored After Shutdown	SYSTEM RST
System Armed	ARMED	System Watchdog Timer Reset	SYSTEM RESET
System Armed STAY Mode	ARMED-STAY	Tamper	TAMPER
System Armed by Downloader	ARMED-REM	Tamper Restore	TMPR RST
System Armed Using Quick-Arm	ARMED-QUICK	Test Report Transmitted	SELF TEST
System Armed with RF Key	ARMED-KEY	User Code Added	Uxxx ADD BY
System Armed Using Schedule	ARMED-AUTO	User Code Changed	Uxxx CHG BY
System Armed Earlier Than Schedule	ARMED-EARLY	User Code Deleted	Uxxx DEL BY
System Armed Later Than Schedule	ARMED-LATE	PTVGM/Access Control Module Fail	ACS MOD
Sys Batt Fail or Disconnection	BATTERY FAIL	PTVGM/Access Control Module Fail Rest	MOD RST
System Battery Restore	LOW BATTERY	Zone Bypass	BYPASS
System Correction of Internal Time	TIME ERROR	Zone Trouble	TROUBLE
System Did Not Arm Using Schedule	MISS ARM	Zone Trouble Restore	TRBL RST

† Occurs after Fire Walk Test activated.

Summary of System Commands

User Code Commands	Add A User Code = User Code + 8 + New User Number + New User's Code Change a Code = User Code + 8 + User Number + New User's Code Delete a User's Code = Your User Code + 8 + User Number to Be Deleted + Your Code Again View User Capability = User's Code + [*] + [*] Set Real-Time Clock (Installer, Master Only) = Code + [#] + 63
Programming Commands	Site Initiated Download = User Code + [#] + 1. Direct-Wire Download Enable = User Code + [#] + 5. Enter Program Mode = Installer Code + 8000. Enter Interactive Program Mode = Installer Code + 8000 + [#] + 93 Exit Program Mode = *99 or *98.
Event Logging Commands	Event Log Display = Code + [#] + 60 (Installer or Master Only) Event Log Print = Code + [#] + 61 (Installer or Master Only) Clear Event Log = Code + [#] + 62 (Installer or Master Only)
Wireless System Commands	House ID Sniffer Mode = Code + [#] + 2 (Installer Only) Transmitter ID Test = Code + [#] + 3 (Installer Only) Go/No Go Test = Code + 5 (Test Key)
Additional Commands	Partition GOTO User Code + [*] + Partition Number 0-8.
	GOTO Home Partition User Code + [*] + 0.
	Panics [*] + 1 or A Key (Zone 995). [*] + [#] or B Key (Zone 999). [#] + 3 or C Key (Zone 996).
	View Downloaded Messages Press 0 for 5 Seconds.
	Display All Zone Descriptors Press [*] for 5 Seconds.
	Display User Self Help Hold Any Key for 5 Seconds.
Output Device Control Commands	Activate Output Device as Programmed = User Code + [#] + 71. Activate Output Device as Programmed = User Code + [#] + 72. Activate Output Device Manually = User Code + [#] + 70. Activate Output Device or System Event Instantly = User Code + [#] + 77.
Scheduling Commands	Installer-Programmed Schedule Events = Installer Code + [#] + 80 (Installer or Master Only). Temporary Schedule Editing = User Code + [#] + 81 (Installer, Master, Manager Only). Extend Closing Time Period = User Code + [#] + 82 (Installer, Master, Manager Only). End User Output Device Programming = User Code + [#] + 83.
Access Control Commands	Activate Access Relay for Current Partition = User Code + 0. Request to Enter/Exit = User Code + [#] + 73. Request to Enter/Exit at Access Point = User Code + [#] + 74 + Access Point Number. Change Access Point State = User Code + [#] + 75 + Access Point + State. Perform a Test of the VistaKey Module = Installer Code + [#] + 78. Perform an Access Control Card Function = User Code + [#] + 79.
Panel Linking Commands	Only user 001 – 050 can perform panel linking. Activate Single-Partition, Single-Panel Mode = User Code + [#] + 86. Exit Single-Partition, Single-Panel Mode = User Code + [#] + 85. Activate Multi-Partition, Multi-Panel Mode = User Code + [#] + 87. Exit Multi-Partition, Multi-Panel Mode = Enter [0]. Activate Multi-Panel View Mode = User Code + [#] + 88. Exit Multi-Panel View Mode = Enter [0].

Index

#80 Scheduling Menu Mode.....	6-4
#93 Menu Mode Programming	4-2
#93 Menu Mode Programming Commands	4-3
12/24 Hour Type Stamp Format.....	5-13
1361	3-12, 3-26, A-1
24 Hour Trouble.....	4-6
24-hour Audible Alarm.....	4-6
24-hour Auxiliary Alarm.....	4-6
24-hour Silent Alarm.....	4-6
2-wire smoke detectors.....	1-1, 3-5
4100SM.....	1-3, 3-16, 7-1, 7-2
4101SN Relay Modules	3-13
4146	1-3, 3-14
4204	1-1, 1-2, 3-5, 3-12, 3-19, 3-21
4285	1-1, 3-18, 3-21, 4
4297	3-7, 3-27
4300	1-2, 3-26, A-1
4-wire smoke detectors.....	3-5, 3-6
5800 series RF.....	3-9, 3-11
5800EU series	3-9, 3-10
5800TM.....	3-10
5827BD.....	3-9, 3-10
5839EU.....	1-1, 3-2, 3-10
5881	1-1, 3-9
5882EU.....	1-1, 3-9
6139	1-1, 3-2, A-1
685 Receiver	3-21
702	3-3
719	3-3
747	3-3

A

AAV.....	3-20, 3-21
AB12M.....	3-3
AC 60Hz or 50Hz	5-12
AC Mains Loss Keypad Sounding	5-2
AC Mains Transformer	3-26
AC Power.....	3-26
Access Group.....	9-3
Access Control.....	3-24, 3-25
Access Control Commands.....	6-8, C-1
Access Control Dialer Enables.....	5-10
Access Control of an Entry/Exit Point	4-8
Access Control of Lighting and Appliances	4-9
Access Control Relay	5-13
Access Control Using RF Transmitter	4-8
Access Point Type 27	4-6
Access Schedules.....	1-3, 6-5
Action Codes.....	6-8
Action Specifier	6-8
Activation Time	6-8
Adding a User Code.....	9-3
Adding an RF Key to a User Code.....	9-4
Addressable Devices	1-1, 3-2
ADEMCO 4+2 EXPRESS.....	A-1
ADEMCO CONTACT ID.....	A-1
ADEMCO HIGH SPEED	A-1
ADEMCO LOW SPEED	A-1
Affects Common Area	5-8

Allow Arming With Faults in Exit Route	5-1
Allow Disarm Outside Window if Alarm Occurs.....	5-14
Allow Disarming Only During Arm/Disarm Windows ..	5-14
ALPHA PROG	4-3
ALT PROGRAM MODE.....	4-1
Antenna Fault	3-18
Arm with Low Battery	5-1
Arm/Disarm Commands	6-8
Arm-Away Type 21.....	4-6
Armed Burglary System T.....	10-2
Arms Common Area	5-8
Arm-STAY Type 20	4-6
ASCII Contact ID Baud Rate	5-7
ASCII Contact ID Reporting with or without ACK	5-7
Audio Alarm Verification.....	1-3, 3-20, 3-21
Auto Arming	6-1
Auto bypass by User	5-9
Auto bypass by Zone	5-9
Auto Bypass Faulted Exit Route Zones	5-9
Auto Bypass Logic	5-8
Auto Disarming	6-1
Auto-Arm Delay.....	2-3, 5-14, 6-1
Auto-Arm Warning.....	5-14, 6-1
Auto-bypass Exit Route Faults	5-1
Auto-Disarm Delay	5-14
Auxiliary Alarm Signaling Equipment.....	3-15
Auxiliary Output Mode	5-11
Auxiliary Power Current Load.....	3-27

B

Back-Up Battery.....	3-27, A-1
Battery Size	3-27
Battery Test.....	10-1
Bell/Siren Relay.....	3-3
Built-in User's Manual	1-4
Burglary Alarm Communicator Delay.....	5-7
Burglary Trigger for Response Type 8.....	5-3
Burglary Walk Test.....	10-1
Button RF (BR) Type 05	3-11, 4-7
Bypass Commands	6-8
Bypass Enable for Fire Zones.....	5-7
Bypass/Unbypass Zones when Armed	5-11

C

Call Waiting Defeat.....	5-11
Callback	7-1
Changing a User Code	9-4
Check Messages.....	10-3
Check or TBLE Display	5-8
Checksum Verification.....	5-5
Chime on External Siren	5-12
Circuit Protectors	A-1
Code + TEST [5]	10-1
COMM. FAILURE.....	10-2
Common Area	1-2, 2-1
Common Area	5-8
Communication Defaults	4-4
Communication Programming Guide	4-4

Index

Communicator Split Reporting Selection	5-10
Compass Downloading Software	7-1
Compatible Polling Loop Devices	3-7
Confirmation of Arming Ding	5-2
Console Input (CS) Type 09	4-7
Contact ID	4-4, B-1
Contact ID Reporting in ASCII Through Printer Port	5-7
Conventions Used in This Manual	vi
CPU Fail Trigger Output	5-11
Cross Zoning Pairs	5-9, 5-10
Cross-Zoning	1-3, 5-9
CUSTOM INDEX	4-3

D

Data Field Descriptions	5-1
Data Field Programming Mode	4-1
Deleting a User Code	9-4
DEVICE PROG	4-3
Dialer Test	10-1
Digital Communicator	A-1
DIP Switch Loop (DP) Type 07	4-7
Direct Wire Downloading	7-2
Disable Download Callback	5-12
Disarm Delay	6-1
Disarm Type 22	4-6
Display Burglary & Panic Alarms for Other Partitions	5-15
Display Fire Alarms of Other Partitions	5-15
Display Mode	3-16
Display Tamper	5-13
Display Troubles of Other Partitions	5-15
Door Status Monitor (DSM) Type 11	4-7
Download Command Enables	5-4
Download ID Number	5-4
Download Phone Number	5-4
Downloader Access Security	7-2
Downloading	1-3, 7-1
Dual Reporting	5-5
Duress Reporting	9-2
Dynamic Signaling Delay	3-17, 5-6
Dynamic Signaling Priority	3-17, 5-6

E

Early Power Detect	3-18
Earth Ground	3-26
ECP Wire Run	3-15
Enable 5800 RF Button Force Arm	5-12
Enable 5800 RF Button Global Arm	5-12
Enable Dialer Reports for Panics & Duress	5-7
Enable Force Arm for Auto-Arm	5-14
Enable GOTO for this Partition	5-14
Enable J7 Triggers for Partition	5-15
Enable Open/Close Report for Installer Code	5-4
Enable Open/Close Report for Keyswitch	5-4
Entering Programming Mode	4-1
Entry Delay #1	5-2
Entry Delay #2	5-2
Entry Warning	5-7
Entry/Exit #1 Burglary	4-5
Entry/Exit #2 Burglary	4-5
EOLR supervision	1-1
Event Log	1-3, 3-16, 5-13, C-1
Event Log and Pager Alpha Descriptors	B-2
Exception Reports	6-1
Exit Delay #1	5-2

Exit Delay #2	5-2
Exit Delay Reset	5-9
Exit Delay Sounding	5-11
Exit Error	1-3
Exiting the User Edit Mode	9-4
Express	4-4
Extend Closing Window	6-1
External Sounders	3-3

F

Final Contact Set	5-1
Fire Display Lock	5-8
Fire With Verification Type 16	4-6
FIRST COMMUNICATION	7-1
First Test Report Time	5-6
Force Arm	6-1
Frwd. Power Loss	3-18
FSA Modules	3-13

G

General Purpose (GP) Type 13	4-7
Glassbreak Detector	1-1, 3-6
Global Arming	1-2, 2-3, 9-3
Go/No Go Test Mode	10-2

H

Hardwired (HW) Type 01	4-7
High Speed	4-4
Holiday Schedule Programming	6-7
Holiday Schedules	1-3, 6-3, 6-4, 6-6
House ID Sniffer Mode	3-10
How to Use Panel Linking	C-1
HSENS	3-8

I

Ignore Expansion Zone Tamper	5-3
Installer (User 1) Code Level 0	9-1
Installer Code	5-1
Installing The Cabinet Lock	3-1
Installing the Control	3-1
Intelligent Test Report	5-3
Interior with Delay	4-6
Interior, Follower	4-6
Intermittent Sensor Suppression	5-7
Internal Clock Sync	5-12
International Date Format	5-12

J

J7 Connector	3-14, 3-21
--------------------	------------

K

Keypad Panics	4-4, 5-3
Keypads	1-1, 3-2
Keyswitch	1-3, 5-2

L

Limitation of Access Schedules	6-2, 6-11
Limitation Of Access Schedules Programming	6-11
LINE SEIZE	A-1
LO BAT	10-3

Log First Maintenance Signal	5-13
Long Range Radios	3-15, 3-17
Low Battery Test Interval	5-10
Low Speed Format	4-4, 5-5
LRR Reporting Options	3-17
LRR Trouble Messages	3-18
LSENS	3-8

M

Macros	1-2
Main Logic Board	3-25
Main Logic Board Supervision Type 28	4-6
Mains Presence Display	5-2
Maintenance Signal Support	3-8
Manager Code Level 2	9-1
Master Code Level 1	9-1
Master Keypad	1-2, 2-4
Maximum Number of Dialler Attempts	5-5
Maximum Number of Zones that can be Bypassed per Partition	5-11
MODEM COMM	7-1, 10-3
Momentary Exit Type 29	4-7
Mounting the PC Board	3-1
Multifrequency Dialling with Pulse Dial Back-up	5-10
Multifrequency or Rotary Dial	5-3
Multi-Panel View Mode	2-7
Multi-Partition Multi-Panel Mode	2-6
Multiple Alarms	5-3
Multiple Partition Access	9-2

N

No Alarm Response Type 23	4-6
Normally Closed or EOLR (Zones 2-8)	5-4
Number of Partitions	5-13
Number of Seconds Added per Day	5-12
Number of Seconds Subtracted per Day	5-12

O

On-Line Control Functions	7-2
Open/Close Reporting	9-2
Open/Close Reports by Exception	5-14, 6-3
Open/Close Schedule Programming	6-6
Open/Close Schedules	1-3, 6-4, 6-5
Open/Close Trigger	3-14
Open/Close Windows	6-8
Operator Codes Levels 3-5	9-1
Output Device Control Commands	C-1
Output Devices	1-2, 3-12
Override AC Loss/Comm Fail	5-15

P

PA400B	3-3
PABX	3-4, 5-3
PAL 328N	14
Panel Linking	2-4, 2-5, 4-9, C-1
Panic Button or Speedkey	5-10
Partitions	1-1, 1-2, 2-1, 2-4, 5-9
Partition-Specific Data Fields	4-2
PassPoint	1-2, 3-25
PassPoint Access Control (ACS) Type 10	4-7
PassPoint Dialer Events	4-8
Perimeter Burglary	4-5
Permanent Keypad Display Backlighting	5-11

Phone Line	3-4, 3-19, 3-21, 3-23
PLL out of Lock	3-18
PLM	2-4
Polling Loop	1-1, 3-7, 3-8, 3-27, 4-7
Power Failure	10-3
Power Unattained	3-18
Powerline Carrier Devices	1-2, 3-19, 3-26
Power-Up in Previous State	5-3
Prevent Fire Timeout	5-3
Prevent Zone XXX Bypass	5-4
Primary Format	5-5
Primary Phone Number	5-4
Primary Subscriber's Account Number	5-4
Print Mode	3-16
Printer Configurations	3-16, 5-13
Priority of Displays for Panel Linking	2-7
Programming	4-1
Programming Commands	C-1
Programming Entry Errors	4-2
Programming Scheduling Options	6-4
Protection zones	4-4
PSTN	1-3

Q

Quick Arm	5-3, 9-1
-----------------	----------

R

RADIONICS LOW SPEED	A-1
Randomise AC Mains Loss Report	5-2
RCVR SETUP ERROR	10-3
Real-Time Clock	8-1
Relay commands	6-8
Relay Timeout XXX Minutes	5-13
Relay Timeout YYY Seconds	5-13
Relay zones	4-4
Remote Keypad Sounder	3-14
Remote Keyswitch	3-14
Remote Point Module	1-1
REPORT CODE PROG	4-3
Report/Log Zone Type 23	5-7
Request to Exit (RTE) Type 12	4-7
Restore Report Timing	5-7
Restrict Disarming	6-1
RF Button	9-3
RF Motion (RM) Type 02	4-7
RF Receiver Supervision Check-in Interval	5-10
RF Transmitter Check-in Interval	5-10
RF Transmitter Low Battery Reporting	5-10
RF Transmitter Low Battery Sound	5-10
RF Troubles	4-7
Ring Detection Count	5-5
RLY VOICE DESCR	4-3
Robofon Version of Contact ID	5-6
RS-485 Bus	2-4, 3-16
RTE	4-7

S

Scheduling	1-3, 6-1, 6-4, C-1
Second Loop Polling Loop (DS) Type 08	4-7
Secondary Format	5-5
Secondary Phone Number	5-4
Secondary Subscriber Account Number	5-7
Security Access Codes	9-1

Index

Selection of Contact ID Message Data on Keypad	
Bus for Subscriber ID #1	5-6
Selection of Contact ID Message Data on Keypad	
Bus for Subscriber ID #2	5-6
Self Activating Siren Output	5-2
Send Cancel If Alarm + Off	5-12
Serial Number Polling Loop (SL) Type 06	4-7
Serial Printer	1-3, 3-16, 7-2
Sescoa/Radionics	4-4, 5-5, A-1
Setting the Time and Date	8-1
Silence Sounder During AAV	5-13
Silent Panic/Duress trigger	3-15
Single-Partition Single-Panel Mode	2-5
Sounder Timeout	5-2
Specifications	A-1
Standard/Expanded Reporting	5-5
Standby Current Drain	3-27
Summer Time Start/End	5-14
Supervised Fire	4-6
Supervised RF (RF) Type 03	4-7
Supervision Pulses for LRR	5-15
Supervisory Zones	4-4
Supplementary Power Supply	3-2
Suppress All Keypad Displays When System is Armed ..	5-7
Suppress Fire Relay	5-4
Suppress Keypad Arming Status Indications	
When System is Armed	5-8
Suppress Status LED Output When Zone 7 Keyswitch	
Enabled/Retain Voltage Trigger Outputs	5-12
Suppress Transmitter Supervision Sound	5-12
Suppress Use of Armed LED on Keypads	5-8
Suppress Wireless Siren Activation for Fire Alarms	5-5
System Commands	C-1
System Communication	B-1
SYSTEM LO BAT	10-1, 10-3
System Messages	10-3
System-Wide Data Fields	4-2

T

Tamper Detect in Test Mode	5-13
TeleCommand	1-1, 5-5
Telephone Module Phone Code	5-2
Telephone Operational Problems	10-3
Telephone System Selection	5-6
Temporary Schedules	6-3, 6-12
Test Report Interval	5-3
Testing The System	10-1
Time Driven Events	1-3, 6-2, 6-7
Time Windows	1-3, 6-2, 6-4, 6-5
TLM Input on Zone 9	5-11
Transformer	3-26
Transmitter Battery Life	3-11
Transmitter ID Sniffer Mode	10-2
Transmitter Supervision	3-11
Transpac receiver	3-23
Trouble by Day/Alarm by Night	4-6
Trouble Messages	10-3
Turning the System Over to the User	10-4

U

UNABLE TO ARM LOBBY PARTITION	2-2
Unsupervised RF (UR) Type 04	4-7
Use Partition Descriptor	5-14
User Bypass of Tamper Faults Instead of Installer	
Only Bypass	5-11
User Code Authority Levels	9-1
User Code Commands	C-1
User Code Rules	9-2
user codes	1-2
User Reset of Tamper Alarms Instead of Installer	
Only Reset	5-11
User Scheduling Menu Mode	6-13
Using ACS Zone Inputs	4-8

V

VA8200	2-4, 3-15
Verified Alarm Report Enable	5-6
Video Alarm Verification (VAV)	1-3, 3-23, 4-10, 5-13
Video Receiver	1-3
Video Transmitter	1-3
View Capabilities	9-1
VIP Module	3-19
VISTA Gateway Module	3-26, 4-8
Vista Interactive Phone Module	3-18
VistaKey	3-24, 4-8
VistaKey Dialer Enables	4-8
Voltage Triggers	1-3

W

Wire Run Length/Gauge	3-2, 3-15
Wireless (RF) Zone Expansion	3-9
Wireless Expansion	1-1
Wireless Keypad Assignment	5-12
Wireless Keypad Tamper Detect	5-11
Wireless System Commands	C-1
Wireless zones	1-1

X

X-10	1-2
XF10	1-2, 3-12, 3-26, A-1
XM10E	1-2, 3-12, 3-26

Z

Zone 5 Audio Alarm Verification	5-13
Zone 8	3-6
Zone 9 Applications	3-6
Zone 9 Response Time	5-2
Zone Index	4-4
Zone Input Type Definitions	4-7
ZONE PROG	4-2
Zone Response Type Definitions	4-5
Zone Type 5 Always Alarm	5-1
Zone Type Restores for Zone Types 1-8	5-6
Zone Type Restores for Zone Types 9, and 10	5-6

Limitations & Warranty

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, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires. 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 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 console (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.

LIMITED WARRANTY

Honeywell International Inc., acting through its Security & Custom Electronics business ("Seller") 165 Eileen Way, Syosset, New York 11791, warrants its product(s) 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(s) or, for product(s) not having a manufacturer's 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(s) 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(s) is altered or improperly repaired or serviced by anyone other than Honeywell factory service. Connection of any device(s) to a communicating bus of a Honeywell security system (e.g., keypad bus, polling loop) other than those manufactured or approved by Honeywell shall void this warranty. For warranty service, return product(s) transportation prepaid, to Honeywell Factory Service, 165 Eileen Way, 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 product(s) it sells may not be compromised or circumvented; that the product(s) will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product(s) will in all cases provide adequate warning or protection. Customer understands that a properly installed and maintained alarm system 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 THAT THE PRODUCT(S) 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(S), 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(s). No increase or alteration, written or verbal, of the obligations of this Limited Warranty is authorized.

Honeywell

165 Eileen Way, Syosset, New York 11791
Copyright © 2006 Honeywell International Inc.

www.honeywell.com/security

EN5944-8ITOŠ

N5944-8IT 7/06 Rev A