VistaKey-SK

Single-Door Access Control Starter Kit

Installation & Setup Guide

K4005 6/00

ADEMCO

Table of Contents

List of Figures

List of Tables

Conventions Used in This Manual

Before you begin using this manual, it is important that you understand the meaning of the following symbols:

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

A checked note includes information you should be aware of before continuing with the installation, and which, if not observed, could result in operational difficulties.

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

Enter Zone Num. (000 = Quit)

You may program many system options by responding to alpha keypad display prompts. These prompts are shown in a box.

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

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

SECTION 1

Introduction

In This Section

General Information

The VistaKey is a single-door access control module that, when connected to a fire/burglary alarm system, provides access control of the protected premises. Multiple VistaKey modules can be used with the alarm system to provide access control to more than one point.

The VistaKey module is part of the VistaKey-SK (Starter Kit). The VistaKey-SK contains all of the components necessary for a minimum access point configuration installation (with exception of mag locks or door strikes).

This Installation and Setup Guide is divided into sections that follow the logical progression of a total VistaKey installation. This section contains general information, lists features, and discusses compatibility issues. The sections that follow provide information about Access Control Integration, Quick Installation, Detailed Installation, Programming, User Commands, System Testing, and an Event Log description.

UL

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

Do NOT use the VistaKey on an alarm panel that is connected to a PassPoint Access Control System via a VISTA Gateway Module.

VistaKey Features

VistaKey features are as follows:

- Each VistaKey communicates with the alarm system control via a special global polling protocol of the Vplex polling loop.
- In the event local power to the VistaKey is lost, the VistaKey module provides backup monitoring of the access point door via a built-in Vplex device that is powered solely from the polling loop. It is programmed as a new type of Vplex device as part of the control's Vplex Device Programming. A serial number label is affixed to the VistaKey module for manual entry of its serial number.
- The VistaKey can handle up to 250 cardholders.
- All configurable options for each VistaKey are accomplished via software, firmware, and nonvolatile memory, eliminating the need for PC board jumpers.

- Access point zone numbers (1-15) are assigned via a user-friendly, 16-position rotary switch.
- The addition and removal of VistaKey modules from the system is easily accomplished via the alarm system keypad.
- The alarm panel event log is expanded to 512 events with the addition of the VistaKey.
- VistaKey events are stored in the alarm panel event log.
- Each VistaKey provides one open collector output trigger (sink 12mA @ 12VDC).
- In the event communication between the VistaKey and the alarm panel is lost for a period of two or more minutes and the VistaKey has power applied, the VistaKey module automatically enters a Reduced Capability Mode (RCM).

The VistaKey also enters the reduced capability mode for two minutes when you have a direct-wire computer connection and you request a download to the alarm panel using the downloader. While in the Reduced Capability Mode, the VistaKey recognizes and grants access for all cards authorized to enter through an access point (without regard to time schedules).

Compatible Fire/Burglary Alarm Systems

The below listing identifies the alarm systems that the VistaKey can interface with, the maximum number of VistaKeys (access points) that can be used with each system, the minimum alarm panel software revision level for compatibility, and software EPROM part numbers.

ALARM SYSTEM	MAXIMUM NUMBER OF VistaKeys	MINIMUM SOFTWARE REVISION LEVEL	EPROM PART NUMBER
VISTA-32FB	4	2.0	WAVIS32FB-12
VISTA-128B	8	2.0	WAVIS128B-12
VISTA-128FB	8	3.0	WAVIS128FB-13
FA1600C	8	7.0	WAVIS150FA-17

You may obtain the software revision level of the alarm panel by entering the program mode and then entering **#92** on the keypad. The second line of the keypad displays the software revision level (without the decimal point).

VistaKey-SK Description

The VistaKey-SK has been designed to provide all components necessary (except door strikes or mag locks) for a minimal configuration access point in one easy-to-install kit. The VistaKey-SK consists of the following components:

- Metal Cabinet
- VistaKey Module
- Distributed Power Supply
- Power Transformer
- Proximity Reader
- Electric Suppressor
- Set of 25 ADEMCO Proximity Access Cards
- Universal Mounting Plate
- Mounting Hardware

Peripheral Devices

The below listing identifies some peripheral devices that can be used with the VistaKey.

DEVICE	DESCRIPTION
Card Reader*	ADEMCO 5365BGP or any equivalent UL listed prox reader with comparable ratings.
Access Cards*	ADEMCO encoded proxcards with 34-bit format. ADEMCO Part Number K3399 (set of 25 cards).
Request to Exit	Pushbutton contact or motion detector such as ADEMCO 998 PIR.
Door Status Monitor	Contact such as ADEMCO TUFFTACTS® Magnetic Reed Contacts.
Power Supply*	Local power supply is ADEMCO part number SA12040.
Door Strike/Mag Lock	Any commercially available electric door strike or magnetic lock with a working voltage of 12VDC and a maximum current of 1.5A. (**NOTE:** Electric deadbolts are not supported.)
Electric Suppressor*	Any commercially available electric suppressor such as the EL-EDS manufactured by EDCO.

* These items are included in the VistaKey-SK.

VistaKey-SK Installation Steps

The installation of a VistaKey-SK consists of a few easy steps for hardware mounting and hook-up, and for programming VistaKey-SK access points via the alarm panel. The steps required are shown in *Figure 1-1: VistaKey Installation Steps*.

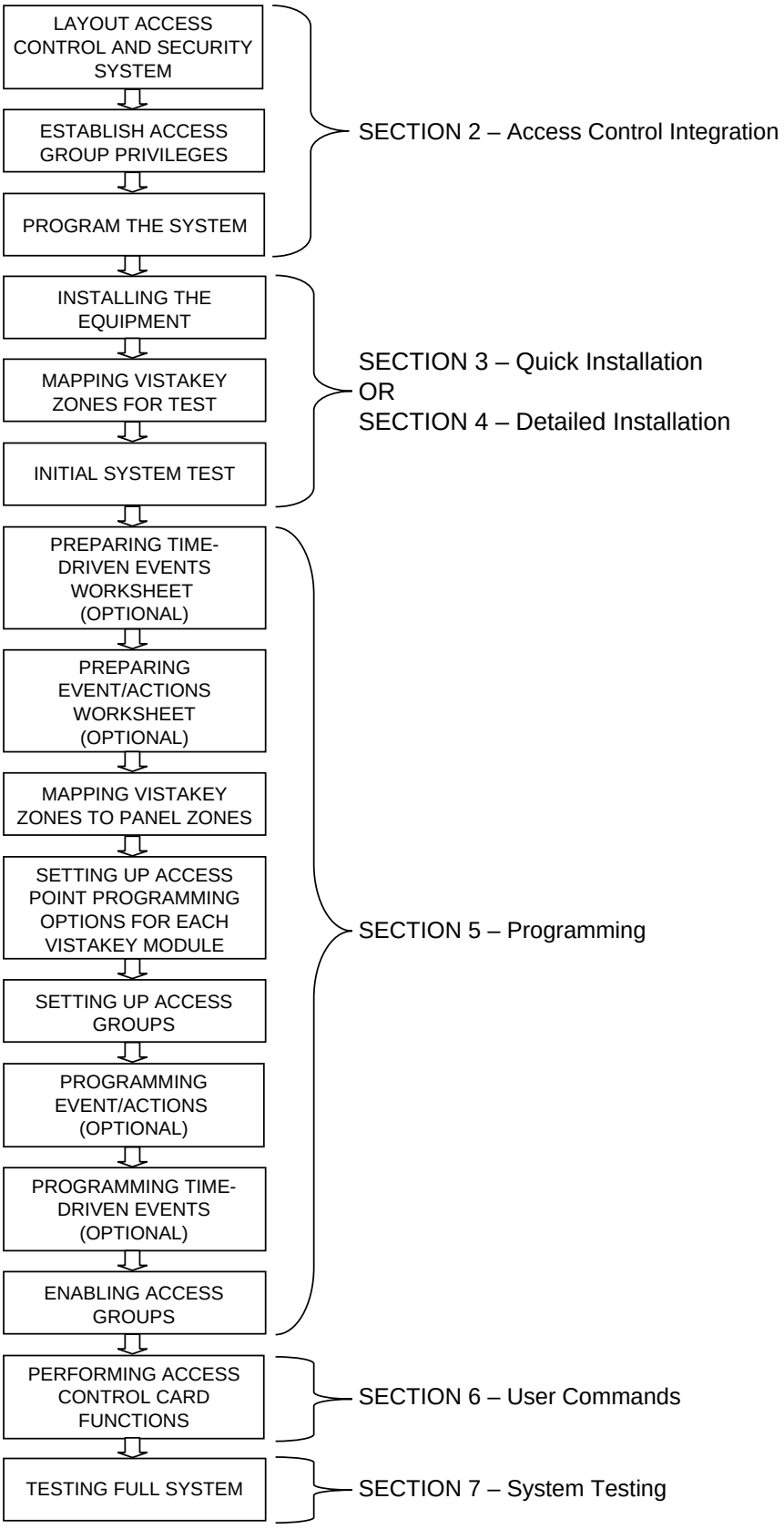


Figure 1-1: VistaKey Installation Steps

SECTION 2

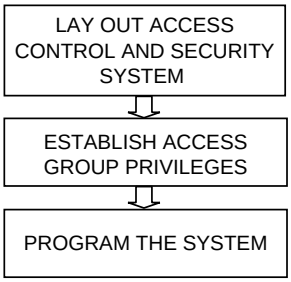
Access Control Integration

In This Section

Introduction

Integrating access control into your fire/burglary security installation requires preliminary considerations as to the placement of devices and the assignment of privileges. This section contains a simple guide for the security system installer to design and implement an elaborate access control and traditional burglary security installation. This section covers, in very simple steps, the fundamental concepts and strategies to install and configure an access control and burglary system. The steps are illustrated with a graphical example of a site layout that uses a VISTA control panel integrated with VistaKey Access Starter Kits.

We recommend that you review this section in its entirety so that you understand the preliminary decisions that need to be made, and that you refer back to this section as needed during the installation and programming of your system.



Overview

The VistaKey access control module is a single-door controller that is easy to install and configure. It supports one proximity card reader with a Weigand-style interface. The system uses the proven ADEMCO 34-bit proximity cards, which, when combined with the VISTA control keypad(s), significantly enhance the security level of the installation. As an integrated access system, the VistaKey gives full and versatile control of employee entrance and egress at all times through a series of programmable time windows and time-driven events. The system can manage up to 250 card users allocated in up to 8 access groups operating a maximum of 8 access points.

Step One – Lay Out Access Control and Security System

The first step to implement an access control/fire burglary security installation is to understand the customer's security needs: the set of conditions and privileges assigned to the occupants or employees based on their status, assignments, and time schedules. This includes interior and perimeter security aspects as well as the flow of occupant movement 24 hours a day, 7 days a week, including holidays, vacations, and plant shutdown periods.

Because security system implementations are not standardized, it is important to determine what access control functions are needed and how they might be integrated into the fire/burglary installation. These concepts will be demonstrated in a series of graphical representations that illustrate the application of the VISTA security system features in the example created.

The following layout shows a typical manufacturing floor plan consisting of office space and assembly or manufacturing area. The layout shows 3 doors as follows:

- Access Point 1 controlled by Reader 1 (at door 1, partition 1).
- Access Point 2 controlled by Reader 2 (at door 2, partition 2).
- Access Point 3 controlled by Reader 3 (at door 3, partition 3)

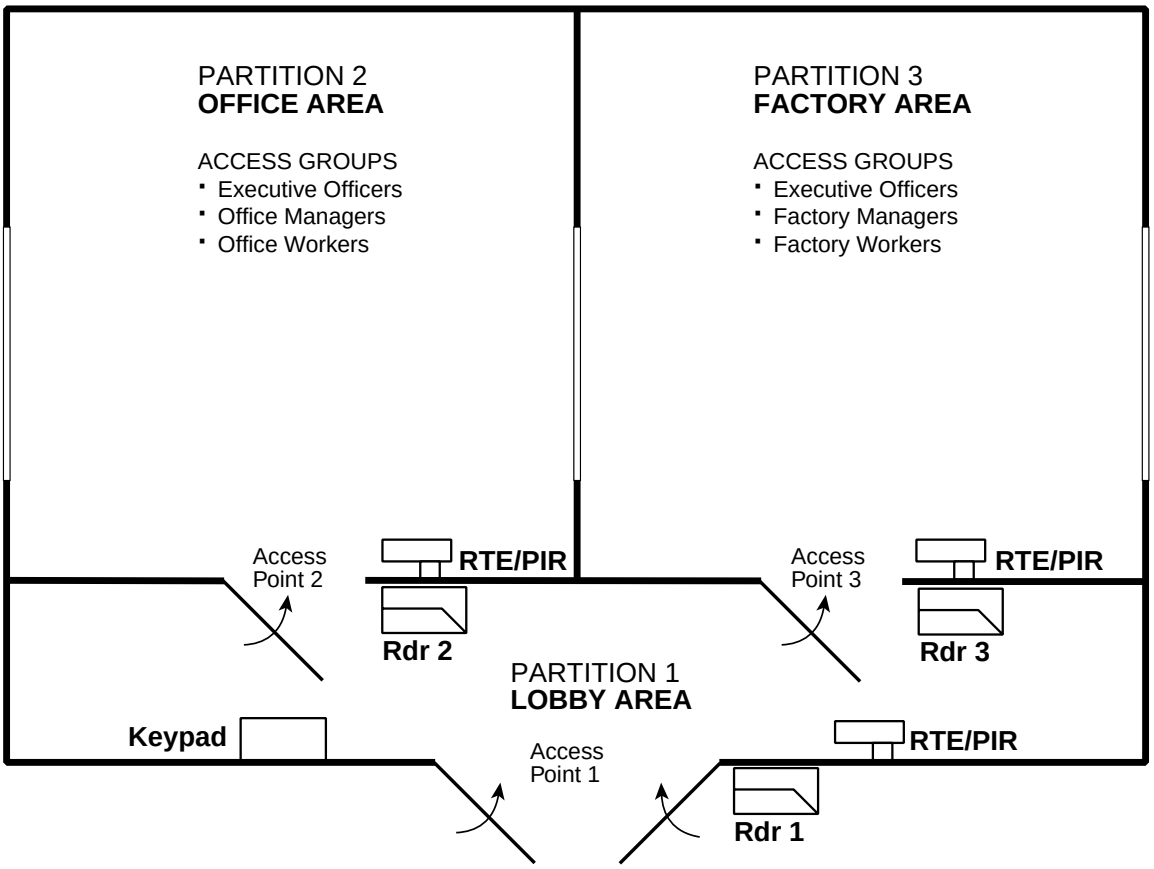


Figure 2-1: Example Floor Plan

The floor plan determines the amount of hardware necessary for the installation. For the floor plan above, the following hardware is required:

- 2 VistaKey-SK Starter Kits each consisting of 1 VistaKey module, 25 access cards, 1 proximity reader, 1 power supply, and 1 cabinet.
- 1 additional VistaKey module to be assembled into one of the Starter Kit cabinets.
- 1 VistaKey-compatible VISTA control (such as a VISTA-128FB).
- 1 additional proximity reader.
- 3 RTE (Request-to-exit) devices such as motion detectors.

- Additional hardware and accessories for the door, window, and interior for burglary and fire protection.

Step Two – Establish Access Group Privileges

Access groups are established based on the site security needs. Once the installer understands these considerations, the next step is to work with the business owner or manager to establish the operating rules that determine how to group the occupants of the premises. Note that the rules of operation should include a detailed flow of movement of personnel throughout the premises. The personnel are divided into access groups that are related to the premises access points and time schedules.

To illustrate this, a list of access groups with corresponding card user authority levels as required by the security needs of the site is provided below. Recall that these security needs are what defines the cardholder's *access privileges*.

- Executive Officers:
  a. Can access all access points.
  b. Can disarm/arm all partitions.
  c. Access 24 hours a day, 7 days a week.
  d. Valid card swipe automatically disarms respective partition.
- Office Managers:
  a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed.
  b. Valid card swipe automatically disarms partitions 1 and 2.
  c. Cannot access point 3 or disarm/arm partition 3.
- Office Workers:
  a. Can access point 1 and arm/disarm partition 1 during time schedule.
  b. Valid card swipe automatically disarms partition 1.
  c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2.
  d. Cannot access point 3 or arm/disarm partition 3.
- Factory Managers:
  a. Can access points 1 and 3 during time schedule while partitions are armed or disarmed.
  b. Valid card swipe automatically disarms partitions 1 and 3.
  c. Cannot access point 2 or disarm/arm partition 2.
- Factory Workers:
  a. Can access point 1 and arm/disarm partition 1 during time schedule.
  b. Valid card swipe automatically disarms partition 1.
  c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3.
  d. Cannot access point 2 or arm/disarm partition 2.

Step Three – Program the System

After the access groups have been defined, we can proceed to fill out the worksheet that facilitates the planning of the security installation. Note that the partial worksheet below will expand as we add more access control/security related requirements specific to our security installation.

Note that an Access Group Worksheet is provided at the end of this section so that you can fill out a worksheet based on your actual site requirements.

In the worksheet below, we have added the names of our access groups (column 2) and added the privileges (column 3) for each group we established in the previous step.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.

Access Points

Description

This portion of step 3 defines which access points (doors) each group will have permission to enter by swiping their valid card at the respective proximity reader.

How this feature is used in our example

This is where we assign access point(s) privileges to each group. Notice that Executive Officers are permitted access through every door in the system, but Factory Workers may only access the lobby door and entry door leading to the factory (points 1 and 3).

Where to program

Program access points in the menu-driven programming mode *93 of the VISTA Panel. See *Setting Up Access Groups* in *Section 5: Programming* later in this guide.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	ACCESS POINTS			
			1	2	3	
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	X	X	X	
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	X	X		
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.	X	X		
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.	X		X	
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.	X		X	

Executive Privilege

Description

Executive Privilege allows a cardholder to access any door in the entire system 24 hours a day, 7 days a week, and gives that card user the ability to automatically disarm any armed partition with a valid card swipe. Executive privilege (status) can be assigned to an individual card user or a group of card users (as in our example system).

How this feature is used in our example

The Officers access group has been assigned Executive Privilege, which permits any of the Officer cardholders to access any door in the system 24 hours a day, and gives them the ability to disarm any armed partition by simply swiping their valid card at any reader.

Where to program

In the VISTA control panel's menu-driven programming mode *93, enable or disable Executive Privilege. See *Setting Up Access Groups* in *Section 5: Programming* later in this guide.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	EXECUTIVE PRIVILEGE
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	X
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.	
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.	
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.	

Armed Restriction

Description

When this function is enabled, it restricts (prevents) a cardholder in an access group from entering an access point when the partition to which it belongs is armed. The card must also not be mapped to a VISTA user who has access to the access point's partition.

Note that Armed Restriction is disabled by default, which means that all cardholders of this group are allowed access to the associated point even if the partition is armed. Consequently, a valid card swipe automatically disarms the partition.

How this feature is used in our example

By enabling Armed Restriction, we have restricted the Office Workers from entering access point 2 and the Factory Workers from access point 3 when those partitions are armed.

Where to program

Enable or disable Armed Restriction in the VISTA control panel's *93 menu-driven programming mode. See *Setting Up Access Groups* in *Section 5: Programming* later in this guide.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	ARMED RESTRICTION (Ptns)			
			1	2	3	4
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.				
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.				
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.		X		
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.				
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.			X	

Time Windows and Timed Events

Description

Using Time Windows in access control is the most efficient way to manage the access control resources and system events. Time windows allow direct and finite control of cardholder access to certain access points by time of day.

How this feature is used in our example

By using time windows and timed events to enable and disable access groups, we are able to control when cardholders are permitted through an access point. As shown in our worksheet below, the Office Managers are allowed to use access points 1 and 2 between the hours of 6:00 AM and 7:00 PM. In fact, all cardholder groups in this example operate under a time window constraint (except for Executive Officers).

Where to program

Program Time Windows and Timed Events in the *#80 Scheduling Mode*. The action selected is 77 Access Group Enable. The action will be enabled during the time window, then disabled outside the specified time window.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	TIME WINDOWS
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	N/A
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	6:00 AM - 7:00 PM
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.	6:00 AM - 7:00 PM
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.	6:00 AM - 11:59 PM
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.	6:00 AM - 11:59 PM

VISTA User Code Authority Level

Description

If unique card tracing is desired, access cards must be assigned a VISTA user code during the card enrollment process. When card trace is enabled, the card grant or deny will be recorded with the VISTA user code in the event log or central station (if programmed). If a card is left at the default value of 000 for the VISTA user number during card enrollment and trace is enabled, that card will report as user U999 in the event log or central station reports(if programmed).

When user codes are programmed into the VISTA security system, authority levels are assigned to them. There are several access control related User Commands (see *Section 6: User Commands* for more details regarding Authorization Levels and access control commands) that should be considered when applying VISTA user code authority levels.

How this feature is used in our example

In our example, we want each cardholder to be uniquely traced. To accomplish this, each card enrolled into our system will also be mapped to a unique VISTA user code that must be programmed into the VISTA panel prior to card enrollment.

- **Executive Officers:** Each Executive officier card has been assigned to a VISTA user code with the authority level of "Master." Having this authority level provides each Executive officer with the ability to use their VISTA user code to access the following access control, output device control, and schedule commands at a VISTA keypad:

  #73, #74, #75, #77, and-#80

  By assigning Executive officiers with an authority level of "Master," they can enroll cards, change card access schedules, etc.

- **Office and Factory Managers:** Each Manager card has been assigned a VISTA user code with the authority level of "Manager." Having this authority level allows each manager the ability to use their VISTA user code to access the following access control commands at a VISTA keypad:

  #73, #74, and #75

  By assigning Managers with an authority level of "Manager," we can prevent them from having the ability to enroll cards, delete cards, or change card access schedules, but they can use their code to bypass or protect access points in the system.

- **Office and Factory Workers:** Each Worker card has been assigned to a VISTA user code with the authority level of "Operator B." Having this authority level allows each worker the ability to use their VISTA user code to access the following access control commands at a VISTA keypad:

  #73 and #74

  By assigning Workers with an authority level of "Operator B," we can prevent them from having the ability to enroll cards, delete cards, change card access schedules, or bypass and protect access points, but they can use their code to request entry or exit through access points in their authorized partition. Also, by using an Operator B authority level, we prevent these workers from bypassing security system protection zones.

Where to program

VISTA user code authority levels are programmed when user codes are entered into the VISTA system. See the VISTA control installation instructions for additional information.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	VISTA USER AUTHORITY LEVEL
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	1 – Master
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	2 – Manager

3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.		4 – Operator B
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.		2 – Manager
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.		4 – Operator B

VISTA User Code Partition Assignment

Description

When VISTA user codes are entered into the VISTA control panel, they can be given access to any or all of the three partitions in our system. Used along with the Armed Restriction feature we discussed earlier, we can control which access points a cardholder can enter if that partition is armed.

How this feature is used in our example

- **Executive Officers** have been assigned a user code that allows access to all partitions. Executive officers have been assigned executive privilege, and although they automatically inherit (by default) all the attributes that allow them to arm/disarm partitions upon a valid card swipe, we recommend programming them as a user in the VISTA system so that they can perform other security system functions.
- **Office Managers** have been assigned a user code that has access to partitions 1 and 2 when armed.
- **Office Workers**, who normally have access to partitions 1 and 2, have been assigned a user code that has access to only partition 1 (when armed). Partition 2 Armed Restriction was previously selected for the office workers preventing them from entering partition 2 when armed.
- **Factory Managers** have been assigned a user code that has access to partitions 1 and 3 when armed.
- **Factory Workers**, who normally have access to partitions 1 and 3, have been assigned a user code that has access to only partition 1 (when armed). Partition 3 Armed Restriction was previously selected for the factory workers preventing them from entering partition 3 when armed.

Where to program

User Code Programming. See VISTA control panel User Guide for more information.

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	VISTA USER CODE (Ptns)		
			1	2	3
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	X	X	X
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	X	X	
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.	X		
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.	X		X
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.	X		

When you have completed all the entries in this example, your worksheet will appear as shown on the following page:

ACCESS GROUP WORKSHEET EXAMPLE

ACCESS GROUP WORKSHEET

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	ACCESS POINTS								EXECUTIVE PRIVILEGE	ARMED RESTRICTION (Ptns)								TIME WINDOWS	VISTA USER AUTHORITY LEVEL	VISTA USER CODE (Ptns)							
			1	2	3	4	5	6	7	8		1	2	3	4	5	6	7	8			1	2	3	4	5	6	7	8
1	Executive Officers	a. Can access all access points. b. Can disarm/arm all partitions. c. Have access 24 hours a day, 7 days a week. d. Valid card swipe automatically disarms respective partition.	X	X	X						X									N/A	1- Master	X	X	X					
2	Office Managers	a. Can access points 1 and 2 during time schedule while partitions are armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 2. c. Cannot access point 3 or disarm/arm partition 3.	X	X																6:00 AM - 7:00 PM	2- Manager	X	X						
3	Office Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 2 only while disarmed and during time schedule. Cannot arm/disarm partition 2. d. Cannot access point 3 or arm/disarm partition 3.	X	X									X							6:00 AM - 7:00 PM	4- Operator B	X							
4	Factory Managers	a. Can access points 1 and 3 during time schedule while partitions armed or disarmed. b. Valid card swipe automatically disarms partitions 1 and 3. c. Cannot access point 2 or disarm/arm partition 2.	X		X															6:00 AM - 11:59 PM	2- Manager	X		X					
5	Factory Workers	a. Can access point 1 and arm/disarm partition 1 during time schedule. b. Valid card swipe automatically disarms partition 1. c. Can access point 3 only while disarmed and during time schedule. Cannot arm/disarm partition 3. d. Cannot access point 2 or arm/disarm partition 2.	X		X									X						6:00 AM - 11:59 PM	4- Operator B	X							

Notes about arming the security system:

In the above example, we have only discussed access control and disarming of the security system. There are several options that may be used to facilitate arming of the security system. They are as follows:

- A key employee or employees may use their user codes to arm the security system.
- A key employee or employees may carry an RF key to facilitate arming of the security system.
- An additional access card may be programmed to arm the security system when swiped at an access point reader by using Event Actions, as discussed in this manual.

Conclusion

The reader is encouraged to study and modify as necessary the example presented in this overview so that it meets the needs of a specific installation.

A worksheet has been provided at the end of this section to facilitate your initial installation.

ACCESS GROUP WORKSHEET

ACCESS GROUP	CARDHOLDERS GROUP	PRIVILEGES	ACCESS POINTS								EXECUTIVE PRIVILEGE	ARMED RESTRICTION (Ptns)								TIME WINDOWS	VISTA USER AUTHORITY LEVEL	VISTA USER CODE (Ptns)							
			1	2	3	4	5	6	7	8		1	2	3	4	5	6	7	8			1	2	3	4	5	6	7	8

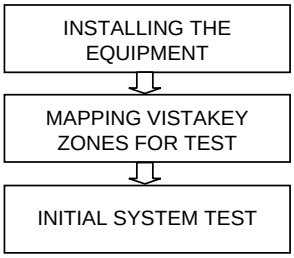
SECTION 3

Quick Installation

In This Section

General Information

This section provides a brief procedure for the initial installation of the VistaKey module. If you require more detailed installation information, please refer to the procedures in *Section 4 – Detailed Installation*. The installation categories described in this section are Installing the Equipment, Mapping VistaKey Zones to Panel Zones, and Initial System Test.



Installing the Equipment

To mount and connect the hardware required to create an access point, perform the steps in the following paragraphs.

Mounting and Connecting

1. The VistaKey uses plug-in terminal blocks for TB-1 and TB3. Keeping the terminal block screws toward the outside edge of the VistaKey printed circuit board, slide the terminal blocks onto the pins extending from the board.
2. When installing a VistaKey-SK, install the mounting plate into the cabinet, mount the cabinet, and install the power supply into the cabinet.

   IMPORTANT: Use the nylon washer supplied on the lower right power supply mounting screw.
3. Mount the VistaKey; door strike or mag lock; and card reader.
4. If applicable, mount the Door Status Monitor (DSM) and/or Request-to-Exit (RTE) devices.
5. Using *Figure 3-1* at the end of this section as a reference, connect the card reader interface cable to TB3, *making the +5V or +12V connection last*.
6. Connect the leads to VistaKey TB1 in the following order:
   a. All ground leads to terminals 2, 5 and 9.
   b. The (optional) DSM, RTE, and General Purpose leads to terminals 6, 7, and 8, respectively.
   c. Door strike (or mag lock) lead to the relay pole terminal 10.
   d. Local +12V supply lead to terminal 1.
   When installing a VistaKey-SK, make this connection from power supply terminal 7.

e. Local +12V supply lead to the N/C relay terminal 11 (if a mag lock is being used); **OR** to the N/O relay terminal 12 (if a door strike is being used).
When installing a VistaKey-SK, make this connection to terminal 11 or 12 from VistaKey TB1 terminal 1.

7. Connect the (–) polling loop and (+) polling loop leads (from the alarm control panel) to terminals 4 and 3, respectively.
8. Set the Address Select switch to the desired access door number (1-15).
9. Repeat steps 2 through 8 for each VistaKey being installed.
10. When installing a VistaKey-SK, connect the transformer output to terminals 1 and 2 of the power supply.
11. Turn on the local +12V to the module by plugging in the VistaKey-SK power transformer. The Reader will beep and its red LED should remain on. *(If the LED is blinking yellow, the state of the DSM switch needs to be temporarily reversed. This may be accomplished by opening the door if closed, or closing the door if opened, until the testing of this access point is completed as described below.)*

Mapping VistaKey Zones for Test

To prepare the VistaKey and panel for testing, VistaKey Zones must be mapped into panel zones. To map VistaKey zones into panel zones, perform the steps below.

1. Enter the **#93 Menu Mode Programming** mode in the alarm system in accordance with the procedures provided in your alarm system manuals. The keypad displays:

ZONE PROG? 1 = YES 0 = NO

2. Press **1** for zone programming. The keypad displays:

Set to Confirm? 1 = YES 0 = NO

3. Press **1** to Confirm. The keypad displays:

ENTER ZONE NO.? 000 = QUIT

4. Enter a 3-digit zone number for the access point (e.g., 100).
5. Press [✲] twice. The keypad displays:

100 ZONE RESPONSE

6. Enter a 2-digit response type such as 01 (Entry/Exit). Press [✲] to accept the entry.
7. Press the [✲] repeatedly until the keypad displays:

100 INPUT TYPE

8. Enter **11** (DSM) and then press [✲] to accept the entry. The keypad displays:

100 Access Point (01-15)

9. Enter a 2-digit access point number corresponding to the access point to be tested. Press [✲] to accept the entry.
10. Press the [✲] repeatedly until the keypad displays:

ENTER ZONE NO.? 000 = QUIT

11. Enter **000** and then press the [✲] to accept the entry. The keypad displays:

QUIT MENU MODE? 1 = YES 0 = NO 0

12. Press **1** to quit the menu mode and then enter **#99** to exit programming.

Initial System Test

ACS access grants and egress grants are alarm type events in the alarm panel log. If you have changed the default values for "Event Log Types" (alarm panel field 1*70) so that alarm type events are not logged, the following procedure can not be used. To use this procedure, refer to the *"Data Field Program Mode"* descriptions in your alarm panel installation and setup guide and temporarily enable alarm type events in field 1*70 to perform this test.

Check the operation of the VistaKey to verify that the installed hardware is functional by performing the following procedure.

1. Using any of the alarm control panel keypads, enter **Installer Code** + **#** + **78**. The keypad displays:

   ```
   ACS TEST MODE
   0 = quit                0
   ```

2. Press **2** on the keypad. The keypad displays:

   ```
   ACS TEST MODE
   GRANT ALL CARDS   2
   ```

3. Press [✲] on the keypad. The keypad starts beeping at a periodic rated indicating the system is in the test mode and the keypad displays:

   ```
   GRANT ALL CARDS
   ACS TEST MODE
   ```

4. Swipe any ADEMCO proximity card past the card reader. If the unit is properly installed, the mag lock or door strike activates, and the green LED temporarily illuminates on the card reader. If the test is successful, advance to step 5. If the mag lock or door strike does not activate, and the green LED does not illuminate, do the following:

   a. Exit the ACS TEST MODE by entering **Installer Code** + **#** + **78** + **0** + *****. The keypad stops beeping and displays:

   ```
   ****DISARMED****
    READY TO ARM
   ```

   b. Check all wiring to the units and that external power is applied.

   c. Return to Step 1 and repeat the test.

5. If additional VistaKeys have been installed for additional access points, repeat step 4 at the card reader for each of the additional access points.

6. Exit the ACS Test Mode by entering **Installer Code** + **#** + **78** + **0** + ***** at the keypad. The keypad stops beeping and displays:

   ```
   ****DISARMED****
    READY TO ARM
   ```

7. Verify that all access points tested are logged in the alarm panel's event log by using the following procedure.

   a. Using any of the alarm panel keypads, enter **Installer Code** + **#** + **60** to view the alarm panel control log. The keypad displays:

   ```
   ENTER 0= RECENT
   1=COMPLETE DUMP
   ```

   b. Press **1** on the keypad. The keypad displays:

   ```
   SCAN LOG BY PART
   0=NO    1-8=PART #
   ```

   c. Press **0** on the keypad. The keypad displays:

   ```
   ALARM  EVENT LOG
   TYPE    CCC UUU
   ```

   d. Press **3** on the keypad repeatedly until the keypad displays:

   ```
   ALL  EVENT LOG
   TYPE    CCC UUU
   ```

   e. Press **8** on the keypad. The keypad display shows the most recent event in the log.

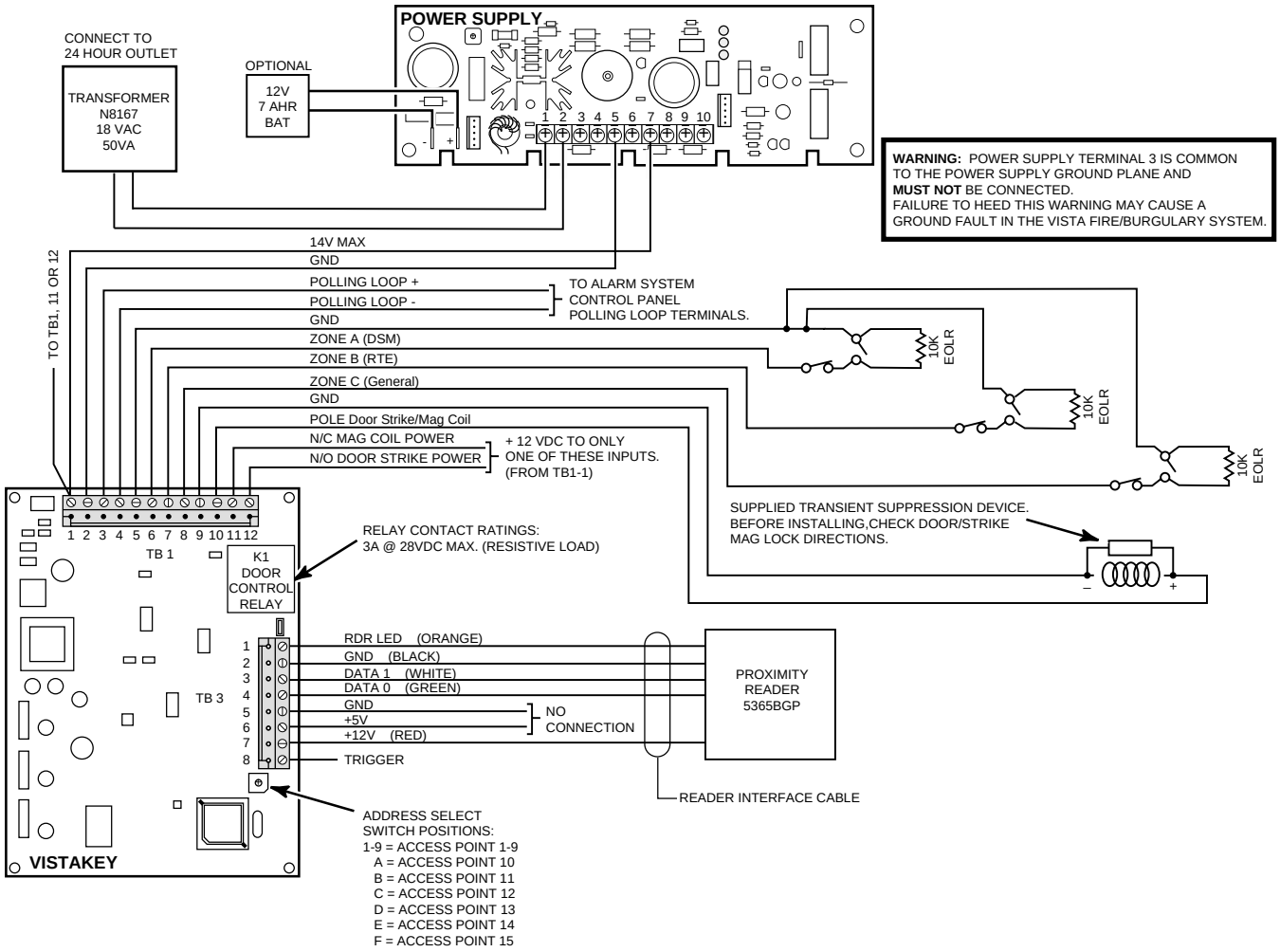
   f. Press **1** on the keypad to step back through the event log to verify that all access points tested are in the log. The first line of the log provides a partition number, date, and time. The second line of the display for the access point test shows "ACS GRT" or "EGR GRT" followed by a 3-digit zone number and user number of U999. Note that U999

indicates a card not linked to a user. If the card was linked to a user, the user number would be displayed.

If an access point shows up incorrectly (e.g., you tested access points (VistaKey addresses) 1 and 2 but the log shows the zone for access point 1 twice), check the address switch setting in the VistaKey for the access point that is missing. If an access point test is missing entirely, recheck the system wiring.

g. Press [*] on the keypad to exit the Log View Mode.

The quick installation is complete and the access point(s) are ready to be programmed into the alarm panel control using the procedures provided in *Section 5: Programming*.



NOTES:

- Local Power and door strike/mag lock power must be supplied from the VistaKey-SK for UL installations.
- Observe the color coding of your reader if not using the ADEMCO reader.
- The use an optional battery on the power supply has not been approved for UL installations.

Figure 3-1: VistaKey Wiring

SECTION 4

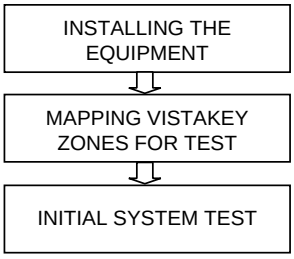
Detailed Installation

In This Section

General Information

This section provides detailed procedures for mounting and connecting the VistaKey-SK or VistaKey module and related devices. The procedures are for one access point, and should be repeated for each additional access point being installed. *Figure 4-1* illustrates what a typical installation looks like. The installation categories described in this section are: Installing the Equipment, Mapping VistaKey Zones for Test, and Initial System Test.

If you have performed the procedures in *Section 3 – Quick Installation*, bypass this section and proceed to *Section 5 – Programming*.



Installing the Equipment

To mount and connect the hardware required to create an access point, perform the steps provided in the following paragraphs.

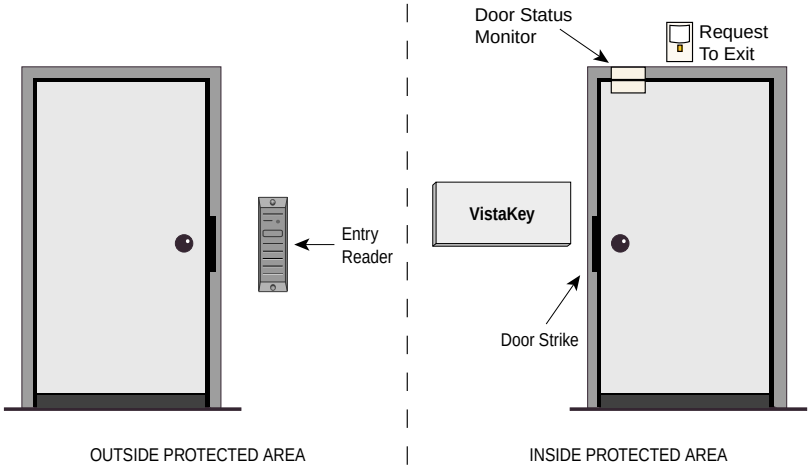


Figure 4-1: Typical VistaKey Installation

Assembling and Mounting the VistaKey-SK

To assemble and mount the VistaKey-SK, follow the procedure below:

1. Determine the mounting location for the VistaKey-SK. It must be mounted inside the protected area near the door strike.
2. Remove the front cover from the VistaKey-SK panel.
3. Mount the Universal Mounting Plate (P/N K4555) in the VistaKey-SK cabinet by sliding the tabs on the rear of the plate into the 3rd row of mounting points in the cabinet. See *Figure 4-2*.

The Universal Mounting Plate is designed so that the tabs will hold it in the cabinet. If desired, retaining screws (supplied) may be used in the middle 2 holes in the plate to attach the plate to the cabinet more securely.

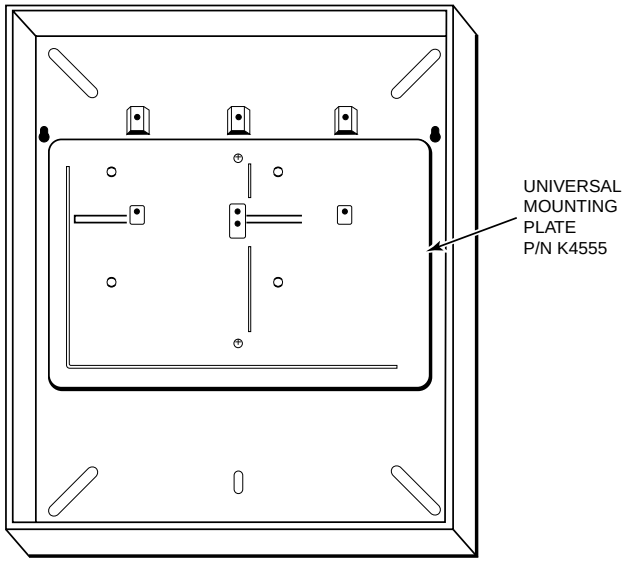


Figure 4-2: Installing the Mounting Plate

4. Position the cabinet on the wall and use the holes in the back of the cabinet to mark your four mounting holes.
5. Using 4 anchors or fasteners (not supplied), mount the cabinet to the wall.
6. Mount the Power Supply (P/N SA12040) in the VistaKey-SK cabinet by sliding it into the slots at the top of the cabinet. Secure the power supply using 3 screws, 3 black mounting spacers, and **1 nylon washer** (on the lower-right screw). See *Figure 4-3*.

Failure to use the nylon washer could result in a ground fault in your fire/burglary system. Disabling the ground fault indication feature is subject to the local authority having jurisdiction.

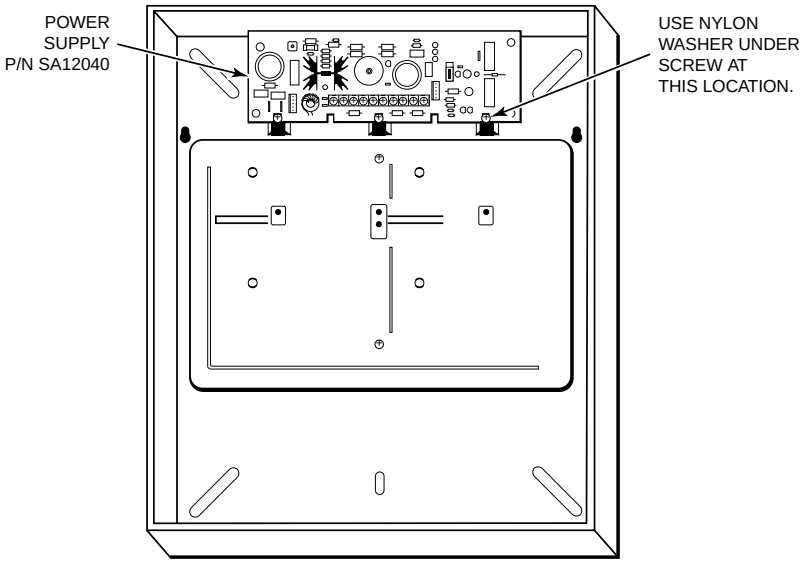


Figure 4-3: Installing the Power Supply

7. Remove the front cover from the VistaKey module.
8. The VistaKey module uses plug-in terminal blocks for TB-1 and TB3. Keeping the terminal block screws toward the outside edge of the VistaKey module printed circuit board, slide the terminal blocks onto the pins extending from the board.
9. Mount the VistaKey module into the cabinet by aligning the slots on the back of the VistaKey module with the pins on the mounting plate and then sliding the VistaKey module to the right. See *Figure 4-4*.

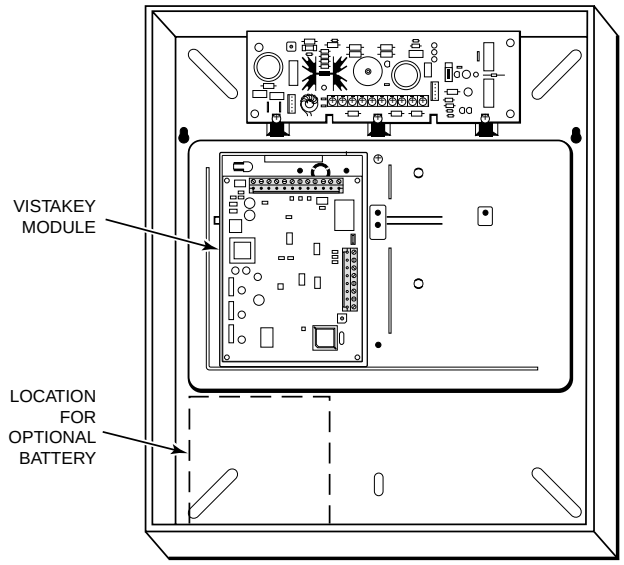


Figure 4-4: Installing the VistaKey module

- Do not re-install the cover of the VistaKey module at this time. The cover is to be re-installed according to instructions in later pages of this manual.
- The area on the right side of the mounting plate may be used for a second VistaKey module.

Mounting and Connecting Card Reader

The card reader is mounted outside the protected area in a location where a cardholder can conveniently swipe a card past the reader. To mount and connect the card reader to VistaKey, follow the procedure below:

Mounting the Card Reader

1. If you are installing the ADEMCO 5365BGP card reader, advance to step 2. If you are installing a different card reader, refer to the diagram on the back of the card reader for the color coding of the card reader wires and their function. Write down this information in the chart below for use in wiring the card reader to the VistaKey.
2. Using the reader as a drilling template, drill two holes in the mounting wall for the reader.
3. Using the mounting hardware included with the reader, secure the reader to the wall.

Connecting the Card Reader

Once the card reader is mounted, you can connect it to the system. Attach the leads from the card reader to the applicable TB3 terminals of the VistaKey as listed below and shown on the Summary of Connections figure at the end of this manual.

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

The reader may have more wires than are used. The unused wires must be insulated from each other and from any other wires or conductive material.

Connecting VistaKey Trigger

The VistaKey has one trigger output (TB3 terminal 8) that can accept a maximum current of 15mA from a source voltage of 12VDC. It is a solid-state digital switch output that may be used to operate small loads such as LEDs and piezoelectric sounders. It can be configured as an output committed to the access point or as an uncommitted output for general use to control the on and off conditions of external devices.

If you are using the VistaKey trigger, connect it to the interfacing device. (Refer to the Summary of Connections diagram at the end of this manual and the instructions provided with the device that the trigger is being connected to.)

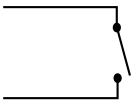
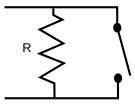
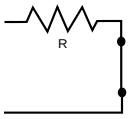
Connecting the VistaKey Zones

The VistaKey contains 3 zone inputs. Each zone may be configured as a supervised (tri-state) or unsupervised (dual-state) input. Zone A is normally used to provide Door Status Monitoring (DSM). Zone B can be configured as the Request to Exit (RTE) input. Zone C serves as a general-purpose zone input that may be used as a tamper input.

The zones can be configured in one of 4 ways:

1. Normally Open
2. Normally Closed
3. End-of-Line Resistor (EOLR) Normally Open
4. End-of-Line Resistor (EOLR) Normally Closed

The following table shows the various configuration options for the VistaKey zone inputs:

	TWO-STATE ZONE (Unsupervised)		**THREE-STATE ZONE (EOLR* Supervised) –Recommended-**	
	Normally Open (N/O)	**Normally Closed (N/C)**	**Normally Open (N/O)**	**Normally Closed (N/C)**
Zone Resistance = 0 (Short)	Fault	Normal	Fault	Trouble
Zone Resistance = Nominal Value	N/A	N/A	Normal	Normal
Zone Resistance = Infinite (Open)	Normal	Fault	Trouble	Fault
Sensor Connections (Sensors shown in ready state)				

* EOLR value is 10KΩ

Door Status Monitoring

A Door Status Monitor (DSM) is a device that will provide a signal while a door (access point) is in the open position. This may be a simple device such as a magnetic contact that is open while the door is open. To use Zone A for door status monitoring, mount the door status monitor device in accordance with the documentation accompanying your DSM. Connect the DSM to the VistaKey TB1 terminal 6 as shown in the Summary of Connections diagram at the end of this manual.

Request to Exit

A Request to Exit (RTE) device is activated to unlock a door (access point) so that you can exit the protected area. Typically, this device may be a PIR or momentary contact switch. To use Zone B for a Request to Exit, mount the Request to Exit device in accordance with the documentation accompanying your RTE. Connect the RTE to the VistaKey TB1 terminal 7 as shown in the Summary of Connections diagram at the end of this manual.

Mounting and Connecting a Door Strike or Magnetic Lock

A door strike or magnetic lock is used to keep an access point locked against unauthorized entry. The door strike or magnetic lock receives power through the VistaKey relay from the power supply.

Do not attempt to provide power for a door strike or magnetic lock from the aux power output of your alarm control panel. Power must be supplied by the VistaKey-SK power supply. Failure to observe this warning could result in damage to your alarm control panel power supply.

Mounting a Door Strike or Magnetic Lock

The procedure for mounting door-locking hardware varies with the type of hardware you plan to use. Refer to the documentation accompanying your door strike or magnetic lock for instructions on performing this step.

Connecting Door Strike or Magnetic Lock

To connect a door strike or magnetic lock, follow the procedure below and refer to the Summary of Connections at the end of this manual.

- We recommend that an electric suppressor such as EL-EDS (manufactured by EDCO and supplied with the VistaKey-SK) be used to provide transient protection for magnetic locks/door strikes and relay contacts. Install the suppressor across the leads connected to the lock as close as possible to the lock.
- Door strikes and magnetic locks may generate electrical noise. Do not route the wiring to the door strike or magnetic lock near any other wiring attached to the VistaKey.

1. Connect the door strike or magnetic lock coil between TB1 terminal 9 (GND) and TB1 (relay pole) terminal 10 (Door Strike/Mag Coil).
2. Connect power to TB1 normally closed (N.C.) terminal 11 if a magnetic lock coil is being used; **OR** to TB1 normally open (N.O.) terminal 12 if a door strike coil is being used as follows:

   When installing a VistaKey-SK and using a +12VDC door strike or mag lock, connect a jumper wire between TB1 terminal 1 and terminal 11 or 12.

Setting the VistaKey Address

The VistaKey is assigned one of 15 access point numbers, or door numbers, from 1 to 9, A, B, C, D, E, or F. This setting must be made before the VistaKey is enrolled into the alarm system.

Note that the VistaKey may be assigned any of 15 access point numbers; however, the total quantity of access points may not exceed the alarm system quantity listed in Section 1 of this manual.

To set the VistaKey address, use a small straight-slot screwdriver to turn the address selection switch to the desired position. Refer to the Summary of Connections diagram at the end of this manual for the switch location. If you are installing more than one VistaKey, the address must be different for each module.

Connecting Polling Loop and VistaKey Power

The final connections to the VistaKey consist of attaching it to the alarm control panel polling loop and connecting the power supply. To make these connections, follow the procedure below and refer to the Summary of Connections at the end of this manual.

1. Connect the VistaKey to the alarm system control using the polling loop + (TB1 terminal 3) and polling loop - (TB1 terminal 4). Refer to the Polling Loop Section in your alarm system Installation and Setup Guide to determine connection points and polarity of the polling loop connections in the alarm system control.
2. Connect VistaKey Power as follows:

   When installing a VistaKey-SK, connect VistaKey TB1 terminal 1 to terminal 7 on the power supply and connect VistaKey TB1 terminal 2 (GND) to terminal 5 on the power

supply. Then, connect the transformer to terminals 1 and 2 of the power supply and plug the transformer into a 24-hour outlet.

When power is connected, the reader will beep and its red LED should remain on. *(If the LED is blinking yellow, the state of the DSM switch needs to be temporarily reversed. This may be accomplished by opening the door if closed, or closing the door if opened, until the testing of this access point is completed as described below.)*

3. Re-install the VistaKey module front cover and, if you are installing a VistaKey-SK, close the door on the VistaKey-SK cabinet.

Mapping VistaKey Zones for Test

To prepare the VistaKey and panel for testing, VistaKey Zones must be mapped into panel zones. To map VistaKey zones into panel zones, perform the following steps:

1. Enter the **#93 Menu Mode Programming** mode in the alarm system in accordance with the procedures provided in your alarm system manuals. The keypad displays:

```
ZONE PROG?
1 = YES   0 = NO
```

2. Press **1** for zone programming. The keypad displays:

```
Set to Confirm?
1 = YES   0 = NO
```

3. Press **1** for Confirm. The keypad displays:

```
ENTER ZONE NO.?
000 = QUIT
```

4. Enter a 3-digit zone number for the access point (e.g., 100).
5. Press the [✲] on the keypad twice. The keypad displays:

```
100 ZONE RESPONSE
```

6. Enter a 2-digit response type such as 01 (Entry/Exit). Press the [✲] to accept the entry.
7. Press the [✲] repeatedly until the keypad displays:

```
100 INPUT TYPE
```

8. Enter **11** (DSM) and then press [✲] to accept the entry. The keypad displays:

```
100 Access Point
(01-15)
```

9. Enter a 2-digit access point number corresponding to the access point to be tested. Press [✲] to accept the entry.
10. Press the [✲] repeatedly until the keypad displays:

```
ENTER ZONE NO.?
000 = QUIT
```

11. Enter **000** and then press the [✲] to accept the entry. The keypad displays:

```
QUIT MENU MODE?
1 = YES   0 = NO          0
```

12. Press **1** to quit the menu mode and then enter **#99** to exit programming.

Initial System Test

ACS access grants and egress grants are alarm type events in the alarm panel log. If you have changed the default values for "Event Log Types" (alarm panel field 1*70) so that alarm type events are not logged, the following procedure can not be used. To use this procedure, refer to the *"Data Field Program Mode"* descriptions in your alarm panel installation and setup guide and temporarily enable alarm type events in field 1*70 to perform this test.

The operation of the VistaKey should be checked to verify that the installed hardware is functional. To perform an initial test of the VistaKey, perform the following procedure.

1. Using any of the alarm panel keypads, enter **Installer Code** + **#** + **78**. The keypad displays:

   ```
   ACS TEST MODE
   0 = quit                 0
   ```

2. Press **2** on the keypad. The keypad displays:

   ```
   ACS TEST MODE
   GRANT ALL CARDS          2
   ```

3. Press [✲] on the keypad. The keypad starts beeping at a periodic rated indicating the system is in the test mode and the keypad displays:

   ```
   GRANT ALL CARDS
   ACS TEST MODE
   ```

4. Swipe any ADEMCO proximity card past the card reader. If the unit is properly installed, the mag lock or door strike will activate, and the green LED will temporarily illuminate on the card reader. If the test is successful, advance to step 5. If the mag lock or door strike does not activate, and the green LED does not illuminate, do the following:

   a. Exit the ACS TEST MODE by entering **Installer Code** + **#** + **78** + **0** + *****. The keypad stops beeping and displays:

      ```
      ****DISARMED****
       READY TO ARM
      ```

   b. Check all wiring to the units and that external power is applied.

   c. Return to Step 1 to repeat the test.

5. If additional VistaKeys have been installed for additional access points, repeat step 4 at the card reader for each of the additional access points.

6. Exit the ACS Test Mode by entering **Installer Code** + **#** + **78** + **0** + ***** at the keypad. The keypad stops beeping and displays:

   ```
   ****DISARMED****
    READY TO ARM
   ```

7. Use the following procedure to verify that all access points tested are logged in the alarm panel's event log.

   a. Using any of the alarm panel keypads, enter **Installer Code** + **#** + **60** to view the alarm control panel log. The keypad displays:

      ```
      ENTER 0= RECENT
      1=COMPLETE DUMP
      ```

   b. Press **1** on the keypad. The keypad displays:

      ```
      SCAN LOG BY PART
      0=NO    1-8=PART #
      ```

c. Press **0** on the keypad. The keypad displays:

ALARM	EVENT LOG
TYPE	CCC UUU

d. Press **3** on the keypad repeatedly until the keypad displays:

ALL	EVENT LOG
TYPE	CCC UUU

e. Press **8** on the keypad. The keypad display shows the most recent event in the log.

f. Press **1** on the keypad to step back through the event log to verify that all access points tested are in the log. The first line of the log provides a partition number, date, and time. The second line of the display for the access point test shows "ACS GRT" or "EGR GRT" followed by a 3-digit zone number and user number of U999. Note that U999 indicates a card not linked to a user. If the card was linked to a user, the user number would be displayed.

   If an access point shows up wrong (e.g., you tested access points (VistaKey addresses) 1 and 2, but the log shows the zone number for access point 1 twice), check the address switch setting in the VistaKey for the access point that is missing. If an access point test is missing entirely, recheck the system wiring.

g. Press the [✲] on the keypad to exit the Log View Mode.

The installation is complete and the access point(s) are ready to be programmed into the alarm control panel using the procedures provided in *Section 5 – Programming*.

SECTION 5

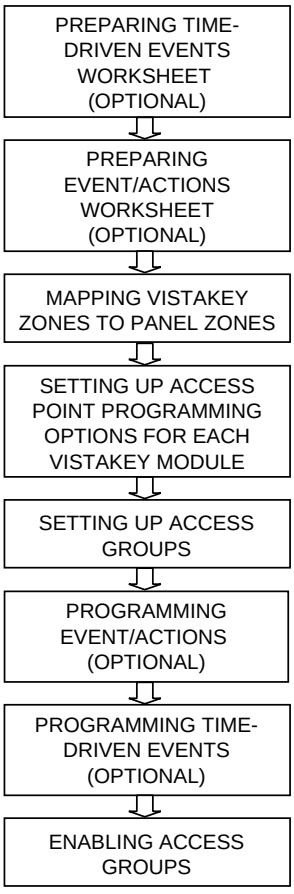
Programming

In This Section

General Information

In order for the system to become operational, the alarm system control panel must be programmed for interaction with the VistaKey zones. This section provides information for programming the operation of the VistaKey with the alarm system control panel.

Programming the VistaKey to operate as a part of the VISTA alarm system can be divided into the following categories.



- **Preparing Time-Driven Events Worksheet** – These paragraphs provide the instructions and codes necessary for filling in the Time-Driven Events Worksheet. Time-driven events are used to make something occur (action) based on a time schedule. This may be used for such things as enabling access groups for entry during working hours only. Note that time-driven events are optional and are not required to operate the system. They are only used to have time (a schedule) cause an action.
- **Preparing Event/Action Worksheet** – These paragraphs provide the instructions and codes necessary for filling in the Event/Action Worksheet. Event/actions are used to make something occur (action) when something happens (event) during a defined time window. One example is turning on a light (via a relay) when anyone is allowed to enter (access grant). Note that event/actions are optional and are not required to operate the system. They are only used to have an event cause an action.
- **Mapping VistaKey Zones to Panel Zones** – The panel Zone Programming procedures are used to define zones in the VISTA alarm panel that will receive information from VistaKey zones. One VISTA alarm panel zone can be mapped to each VistaKey zone.
- **Setting Up Access Point Programming Options** – Access Point Programming procedures are used to define the parameters for each of the VistaKey zones, including which group(s) have access through an access point (door).
- **Setting Up Access Groups** – These paragraphs describe how to define the capabilities (privileges) for each group of users.
- **Programming Event/Actions** – These paragraphs describe how to program the information from your Event/Actions Worksheet into the alarm panel. Event/actions are used to make something occur (action) when something happens (event). Note that event/actions are optional and are not required to operate the system. They are only used to have an event cause an action.
- **Programming Time-Driven Events** – These paragraphs describe how to program the information from your Time-Driven Events Worksheet into the alarm panel. Time-driven events are used to make something occur (action) based on time. Note that time-driven events are optional and are not required to operate the system. They are only used to have time cause an action.
- **Enabling Access Groups** – Newly defined access groups must be enabled before they become active. Access Groups can be enabled by the next applicable time window that becomes active or by the #77 command for an instant enable.

- The term *access groups* within this document refers to *access point groups*. It should not be confused with the access groups to which user codes are assigned as discussed in your alarm panel manuals.
- For additional information on programming procedures, refer to the manuals provided with the alarm system.

Preparing a Time-Driven Events Worksheet

The Time-Driven Events Worksheet is used to prepare a set of schedules used to activate outputs, bypass zones, etc. based on a time schedule. Twenty such events may be programmed for the system, each event governed by the previously defined time windows.

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

- When you use action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only), these actions disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.
- The time-driven events described here are the same as those explained in your alarm panel Installation and Setup Guide, except that additional actions have been added. If you are already using time-driven events, make certain that the first Timed Event # you use is after the last number you have already assigned; otherwise you will overwrite your existing time-driven events.
- At the end of a time window controlling an access point, the access point will revert to the protect mode.

Fill out the Time-Driven Events Worksheet (near the end of this section) using the steps outlined below:

As an aid to understanding the procedures for filling out the Time-Driven Events Worksheet, assume that you want to enable access groups 1 and 2 from 08:00 AM to 05:00 PM (set via time window 01) on Monday through Friday. As you perform the following steps, examples are provided for filling out the worksheet.

1. **Enter the Action No. listed in *Table 5-1: Action Codes* for the action desired.**

   *Example: Enter Action No. **77** for Access Group Enable.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	***77***												
2													

2. **Enter the Action Name listed in *Table 5-1: Action Codes* for the action number.**

   *Example: Enter **ACS Grp Enbl** for Access Group Enable.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	*77*	***ACS Grp Enbl***											
2													

3. **Enter the Action Specifier that corresponds to the description in *Table 5-1: Action Codes*.**

   *Example: Enter **1** and **2** for access groups 1 and 2.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	*77*	*ACS Grp Enbl*	***1 2***										
2													

4. **Enter the Time Window number that corresponds to the time window (previously programmed) that should trigger the action.**

   *Example: Assume that time window 01 has a start time of 08:00 AM and end time of 05:00 PM. Enter **01** for time window 1.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	*77*	*ACS Grp Enbl*	*1 2*	***01***									
2													

5. **Enter the Activation Time that is desired for the action. Activation times are as follows:**

   1 =Beginning of time window
   2 =End of time window
   3 =During time window active period only (on at beginning of window, off at end).
   4 =Beginning and end of time window

   *Example: Enter **3** so that the access groups will be enabled for the full period of the time window.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	*77*	*ACS Grp Enbl*	*1 2*	*01*	***3***								
2													

6. **Place an X under each Day that the action is to occur within the time window Specified. Note that when Holiday is selected, it will over-ride the day of the week selection (e.g., Holiday is selected and the holiday falls on Saturday but Saturday is not selected, the Holiday selection makes the action occur). For additional information, refer to Holiday Schedules in your alarm system manual.**

   *Example: Enter an **X** under M, T, W, T, and F for Monday through Friday.*

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1	*77*	*ACS Grp Enbl*	*1 2*	*01*	*3*	***X***	***X***	***X***	***X***	***X***			
2													

   Following the example above, access groups 1 and 2 will be granted access between the hours of 08:00 AM and 05:00 PM on Monday through Friday.

Table 5-1: Action Codes

ACTION NO.	ACTION NAME	ACTION SPECIFIER	ACTION DESCRIPTION
Relay Commands Activation times **1** (Beginning), **2** (End), **3** (During) are the only valid choices for relay commands. "During" can be used to control the relay for a specific time only. For example, if "during" is selected with Relay On, the system will automatically energize the relay at the beginning of the window and automatically de-energize the relay at the end of the window.			
01	Relay On	Relay #	Relay On – Turn on relay indicated by the specifier
02	Relay Off	Relay #	Relay Off – Turn off relay indicated by the specifier
03	Rly On 2 Sec	Relay #	Relay Close for 2 seconds – Close relay indicated by the specifier for 2 seconds
04	Relay xx Min	Relay #	Relay Close XX minutes – Close relay indicated by the specifier for XX minutes (XX minutes set in field 1*74)
05	Relay yy Sec	Relay #	Relay Close YY seconds – Close relay indicated by specifier for YY seconds (YY seconds set in field 1*75)
06	Rly Grp On	Relay Group #	Relay Group On – Turn on relay group indicated by specifier
07	Rly Grp Off	Relay Group #	Relay Group Off – Turn off relay group indicated by the specifier
08	Rly Grp 2 Sec	Relay Group #	Relay Group Close for 2 seconds – Close all relays in the group indicated by the specifier for 2 seconds
09	Rly Grp xx Min	Relay Group #	Relay Group Close XX minutes – Close relay group indicated by the specifier for XX minutes (XX minutes set in field 1*74)
10	Rly Grp yy Sec	Relay Group #	Relay Group Close YY seconds – Close relay group indicated by the specifier for YY seconds (YY seconds set in field 1*75)
Arm/Disarm Commands Activation times **1** (Beginning), **2** (End), **3** (During) are the only valid choices for automatic arming and disarming functions. "During" can be used to arm or disarm the control for a specific time only. For example, if "during" is selected with Arm-STAY, the system will automatically Arm-STAY at the beginning of the window and automatically disarm at the end of the window.			
20	Arm STAY	Partition(s)	Arm STAY – Arm the partition(s) indicated by the specifier in the STAY mode
21	Arm AWAY	Partition(s)	Arm AWAY – Arm the partition(s) indicated by the specifier in the AWAY mode
22	Disarm	Partition(s)	Disarm – Disarm the partition(s) indicated by the specifier
23	Force Arm STAY	Partition(s)	Force Arm STAY – Force arm the partition(s) indicated by specifier in the STAY mode (auto-bypass faulted zones)
24	Force Arm AWAY	Partition(s)	Force Arm AWAY – Force arm the partition(s) indicated by the specifier in the AWAY mode (auto-bypass faulted zones)
Bypass Commands Activation times **1** (Beginning), **2** (End), **3** (During) are the only valid choices for bypass commands. If **3** (During) is selected for auto-bypassing, the system will bypass the zone(s) specified on a particular zone list at the beginning of the window and unbypass the zone(s) at the end of the window. If it is selected for auto unbypassing, the system will remove the bypass of the zone(s) at the beginning of the window and will restore the bypass of the zone(s) at the end of the window.			
30	Bypass Zn List	Zone list #	Auto bypass zone list – Automatically bypass the zone list indicated by the specifier
31	Unbyps Zn List	Zone list #	Auto unbypass zone list – Automatically unbypass the zone list indicated by the specifier
Open/Close Windows Activation time **3** (During) is the only valid choice for these commands. When using Enable Open Window, Enable Close Window, and Enable Access Window, the window is active for the partitions selected by the specifier except as follows: • When an Event/Action occurs that would disable a window (partition not selected), the window for the partition is only disabled if it is not currently enabled by a timed method (e.g., O/C schedule, Time-Driven Event, Access Schedule). • When a timed window (e.g., O/C schedule, Time-Driven Event, Access Schedule) occurs that would disable a window (partition not selected), the window for the partition is only disabled if it is not currently enabled by an Event/Action.			
40	En Open Wind	Partition(s)	Enable Opening Window by partition – Enable the opening window for the partition indicated by the specifier (used to control central station reporting - see Open/Close Reports by Exception in your alarm system manual for additional information)

Table 5-1: Action Codes (cont'd)

ACTION NO.	ACTION NAME	ACTION SPECIFIER	ACTION DESCRIPTION
Open/Close Windows (cont'd)			
41	En Close Wind	Partition(s)	Enable Closing Window by partition – Enable the closing window for the partition indicated by the specifier (used to control central station reporting - see Open/Close Reports by Exception in your alarm system manual for additional information)
42	En Access Wind	Access Group	Enable Access Window for user access group – Enable the access window for the user access group indicated by the specifier (enables user arming or disarming - see Limitation of Access Schedules in your alarm system manual for additional information)
50	Off-Normal Reminder	None	Off-Normal Reminder – All keypads with a fire zone that is in an off-normal state will begin beeping until the condition is acknowledged by the user
Access-Related Actions All access-related actions are active during the time window and you will not be presented with a prompt requesting an activation time.			
55	AP Grant	Access Point #	Access Point Grant – Grant access at access point indicated by specifier
56	AP Grant/O	Access Point #	Access Point Grant with Override – Grant access with override at access point indicated by specifier
57	AP Protect	Access Point #	Access Point Protect – Protect access point indicated by specifier
58	AP Bypass	Access Point #	Access Point Bypass – Bypass access point indicated by specifier
59	AP Lock	Access Point #	Access Point Lock – Lock access point indicated by specifier
60	AP Exit Only	Access Point #	Access Point Exit Only – Put access point indicated by specifier in Exit Only mode
61	AP Grp Grt	Group #	Access Point Group Grant – Grant access to all access points that belong to access group(s) indicated by specifier
62	AP Grp Grt/O	Group #	Access Point Group Grant with Override – Grant access with override to all access points that belong to access group(s) indicated by specifier
63	AP Grp Prot	Group #	Access Point Group Protect – Put all access points that belong to access group(s) indicated by specifier in Protect mode
64	AP Grp Bypas	Group #	Access Point Group Bypass – Put all access points that belong to access group(s) indicated by specifier in Bypass mode
65	AP Grp Lock	Group #	Access Point Group Lock – Put all access points that belong to access group(s) indicated by specifier in Locked mode
66	AP Grp Exit O	Group #	Access Point Group Exit Only – Put all access points that belong to access group(s) indicated by specifier in Exit Only mode
67	AP Ptn Grt	Partition #	Access Point Partition Grant – Grant access to all access points that belong to partition(s) indicated by specifier
68	AP Ptn Grt/O	Partition #	Access Point Partition Grant with Override – Grant access with override to all access points that belong to partition(s) indicated by specifier
69	AP Ptn Prot	Partition #	Access Point Protect by Partition – Protect all access points that belong to partition(s) indicated by specifier
70	AP Ptn Bypas	Partition #	Access Point Bypass by Partition – Bypass all access points that belong to partition(s) indicated by specifier
71	AP Ptn Lock	Partition #	Access Point Lock by Partition – Lock all access points that belong to partition(s) indicated by specifier
72	AP Ptn Exit O	Partition #	Access Point Exit Only by Partition – Put all access points that belong to partition(s) indicated by specifier into Exit Only mode
73	AP Trg On	Access Point #	Access Point Trigger On – activate trigger on access point indicated by specifier (NOTE: This action code can be used with the #77 command and with Event/Actions ONLY. It must not be used with Time-Driven Events.)
74	AP Trg Off	Access Point #	Access Point Trigger Off – De-activate trigger on access point indicated by specifier (NOTE: This action code can be used with the #77 command and with Event/Actions ONLY. It must not be used with Time-Driven Events.)
77	ACS Grp Enbl	Group #	Access Point Group Enable – Enable access group(s) indicated by specifier (enables a group's cardholders so that valid access requests are accepted)
78	ACS Grp Dsbl	Group #	Access Point Group Disable – Disable access group(s) indicated by specifier

Preparing an Event/Actions Worksheet

Event/actions are events used to activate outputs, bypass zones, etc. based on the events that occur in the alarm system. There are 32 event/actions that may be programmed for the system.

The actions that can be programmed to automatically occur due to (or as a result of) set events are: relay commands, arm/disarm commands, zone bypassing commands, open/close access conditions, and access control commands.

Fill out the Event/Action Worksheet (located at the end of this section) using the steps outlined below:

As an aid to understanding the procedures for filling out the Event/Actions worksheet, assume that you want to turn on a light (via relay # 1) on an access grant at access point 1, and further assume that this is to occur between the hours of 08:00 AM and 05:00 PM (set via time window 01) on Monday through Friday. As you perform the following steps, examples are provided for filling out the worksheet.

1. **Enter the Event No. listed in *Table 5-2: Event Actions* for the event desired.**

   *Example: Enter Event No. **22** for an access point grant.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	***22***														
2															

2. **Enter the Event Name listed in *Table 5-2: Event Actions* for the event number.**

   *Example: Enter **AP Grt** for event number 22.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	***AP Grt***													
2															

3. **Enter the Event Specifier that corresponds to the description in *Table 5-2: Event Actions*.**

   *Example: Enter **01** for access point number.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	***01***												
2															

4. **Enter the Action No. listed in *Table 5-1: Action Codes* for the action desired.**

   *Example: Enter Action No. **01** for relay on.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	*01*	***01***											
2															

5. **Enter the Action Name listed in *Table 5-1: Action Codes* for the action number.**

   *Example: Enter **Relay On** for action number 01.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	*01*	*01*	***Relay On***										
2															

6. Enter the Action Specifier that corresponds to the description in *Table 5-1: Action Codes.*

*Example: Enter **01** for relay number 1.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	*01*	*01*	*Relay On*	***01***									
2															

7. Enter the Time Window number that corresponds to the time window (previously programmed) for the time period during which the event should trigger the action.

*Example: Assume that time window 01 has a start time of 08:00 AM and end time of 05:00 PM. Enter **01** for time window 1.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	*01*	*01*	*Relay On*	*01*	***01***								
2															

8. Place and X under each Day that the event/action is to occur within the time window specified. Note that when Holiday is selected, it will over-ride the day of the week selection (e.g., Holiday is selected and the holiday falls on Saturday but Saturday is not selected, the Holiday selection makes the event/action occur). For additional information, refer to Holiday Schedules in your alarm system manual.

*Example: Enter an **X** under M, T, W, T, and F for Monday through Friday.*

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1	*22*	*AP Grt*	*01*	*01*	*Relay On*	*01*	*01*	***X***	***X***	***X***	***X***	***X***			
2															

Following the example above, the access grant at access point 1 (event) turns on relay # 1 (action).

9. Repeat steps 1 through 8 for each event/action desired.

Table 5-2: Event Actions

EVENT NO.	EVENT NAME	EVENT SPECIFIER	EVENT DESCRIPTION
Partition (Ptn) Specifiers			
00	None	None	Not Used
01	Arm Ptn	Partition(s)	Arm Partition – Any partition indicated by specifier was armed
02	Disarm Ptn	Partition(s)	Disarm Partition – Any partition indicated by specifier was disarmed
03	Fire Ptn	Partition(s)	Fire Partition – Any partition indicated by specifier went into fire alarm
04	Fire Rst Ptn	Partition(s)	Fire Restore Partition – Any partition indicated by specifier has been fire restored
05	Burg Ptn	Partition(s)	Burglary Partition – Any partition indicated by specifier has gone into burglar alarm
06	Burg Rst Ptn	Partition(s)	Burglary Restore Partition – Any partition indicated by specifier has been burglar alarm restored
07	Alm Ptn	Partition(s)	Alarm Partition – Any partition indicated by specifier has gone into alarm
08	Alm Rst Ptn	Partition(s)	Alarm Restore Partition – Any partition indicated by specifier has been alarm restored
09	Dur Ptn	Partition(s)	Duress Partition – Any partition indicated by specifier has gone into duress
10	Dur Rst Ptn	Partition(s)	Duress Restore Partition – Any partition indicated by specifier has been duress restored
11	Trb Ptn	Partition(s)	Trouble Partition – Any partition indicated by specifier has gone into trouble
12	Trb Rst Ptn	Partition(s)	Trouble Restore Partition – Any partition indicated by specifier has been trouble restored
13	Byp Ptn	Partition(s)	Bypass Partition – Any partition indicated by specifier has a zone that's been bypassed
14	Byp Rst Ptn	Partition(s)	Bypass Restore Partition – Any partition indicated by specifier has a zone that's been unbypassed
15	Late Disarm Ptn	Partition(s)	Late Disarm Partition – Any partition indicated by specifier was late in disarming
16	Early Arm Ptn	Partition(s)	Early Arm Partition – Any partition indicated by specifier was armed early
17	Fail Arm Ptn	Partition(s)	Fail Arm Partition – Any partition indicated by specifier failed to arm on time
User Specifiers			
18	Arm Usr	VISTA User #	Arm User – User indicated by specifier armed a partition
19	Disarm Usr	VISTA User #	Disarm User – User indicated by specifier disarmed a partition
20	Grt Usr	VISTA User #	Grant User – User indicated by specifier was granted access
Card ID Specifiers			
21	Grant Card	Card ID #	Grant Card – Card ID indicated by specifier was granted access
Access Point (AP) Specifiers			
22	AP Grt	Access Point #	Access Point Grant – Access point indicated by specifier granted access
23	AP Deny	Access Point #	Access Point Deny – Access point indicated by specifier denied access
24	AP Byp	Access Point #	Access Point Bypass – Access point indicated by specifier was bypassed
25	None	None	Not Used
26	AP Lock	Access Point #	Access Point Lock – Access point indicated by specifier was locked
27	AP Prot	Access Point #	Access Point Protect – Access point indicated by specifier was put in Protect mode
28	None	None	Not Used
29	AP Grt Ovr	Access Point #	Access Point Grant Override – Access point indicated by specifier is doing a grant with override
30	Dur Grt	Access Point #	Access Point Duress Grant – Access point indicated by specifier is granting under duress
31	Prop Opn Alm	Access Point #	Access Point Prop Open Alarm – Access point indicated by specifier is in prop alarm
32	Prop Opn Rst	Access Point #	Access Point Prop Open Restore – Access point indicated by specifier has restored prop alarm

Table 5-2: Event Actions (cont'd)			
EVENT NO.	**EVENT NAME**	**EVENT SPECIFIER**	**EVENT DESCRIPTION**
Access Point (AP) Specifiers (cont'd)			
33	Force Opn	Access Point #	Access Point Force Open – Access point indicated by specifier is in door forced open alarm
34	Force Rst	Access Point #	Access Point Force Open Restore – Access point indicated by specifier has restored door forced alarm
Zone Number Specifiers			
35	Fire Zn	Zone #	Fire Zone – Zone indicated by specifier has gone into fire alarm
36	Fire Rst Zn	Zone #	Fire Restore Zone – Zone indicated by specifier has restored its fire alarm
37	Burg Zn	Zone #	Burglary Zone – Zone indicated by specifier has gone into burg alarm
38	Burg Rst Zn	Zone #	Burglary Restore Zone – Zone indicated by specifier has restored burg alarm
39	Alm Zn	Zone #	Alarm Zone – Zone indicated by specifier has gone into alarm
40	Alm Rst Zn	Zone #	Alarm Restore Zone – Zone indicated by specifier has restored its alarm
41	Trb Zn	Zone #	Trouble Zone – Zone indicated by specifier has gone into trouble
42	Tble Rst Zn	Zone #	Trouble Restore Zone – Zone indicated by specifier has restored its trouble
43	Byp Zn	Zone #	Bypass Zone – Zone indicated by specifier has been bypassed
44	Byp Rst Zn	Zone #	Bypass Restore Zone – Zone indicated by specifier has been unbypassed
Arming Specifiers			
45	Arm Stay Ptn	Partition(s)	Arm Stay Partition – Any partition indicated by specifier has gone into armed-Stay
46	Arm Away Ptn	Partition(s)	Arm Away Partition – Any partition indicated by specifier has gone into armed-Away
47	Arm Inst Ptn	Partition(s)	Arm Instant Partition – Any partition indicated by specifier has gone into armed-Instant
48	Arm Max Ptn	Partition(s)	Arm Maximum Partition – Any partition indicated by specifier has gone into armed-Max
49	Arm Stay Usr	VISTA User #	Arm Stay User – User indicated by specifier armed a partition in Stay mode
50	Arm Away Usr	VISTA User #	Arm Away User – User indicated by specifier armed a partition in Away mode
51	Arm Inst Usr	VISTA User #	Arm Instant User – User indicated by specifier armed a partition in Instant mode
52	Arm Max Usr	VISTA User #	Arm Maximum User – User indicated by specifier armed a partition in Max mode

Mapping VistaKey Zones to Panel Zones

You will be dealing with four zone types when mapping VistaKey zones to panel zones. As an aid to understanding the programming steps required, a brief description of these four zone types follows:

- DSM – This zone type is used to map an access point to a zone and is used to monitor the status of an access point (e.g., open, closed). When the access point is bypassed, the controlled door is propped, or the controlled door is forced, the DSM operates according to the zone response type. The DSM device is normally a magnetic switch mounted on the door. The status of the switch is different while the door (access point) is in an open condition.
- RTE – This zone type is used to map an uncommitted RTE zone to an alarm panel zone. This input type is not normally used if the RTE zone is being used for a request to exit function. The RTE device may be something as simple as a momentary contact switch or as complex as a motion detector.

- GP – This maps the GP zone to an alarm panel zone. This zone operates in the same manner as other VISTA 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 alarm panel. This zone is normally used for tamper in installations requiring supervision of the cabinet cover.
- DSMB – The DSMB is a Serial Polling Loop input type zone that maps the SIM in the VistaKey to an Alarm Panel zone. In the event local power to the VistaKey is lost, the status of the DSM can no longer be reported to the panel via the normal microprocessor circuits of the VistaKey. In this case a Vplex SIM, which is located on the VistaKey board and powered directly from the polling loop, is activated and reports the state of the DSM via the standard Vplex polling system.

To program the VISTA Alarm Panel for VistaKey operation, enter #**93 Menu Mode Programming** in the alarm system in accordance with the procedures provided in your alarm system manuals. When you enter **#93 Menu Mode Programming**, the following message is displayed on the keypad:

```
ZONE PROG?
1=YES   0=NO
```

Press **1** to enter Zone Programming. The following screen appears.

NOTE: During programming, press [✲] to display the next screen. Press [**#**] to display a previous screen.

```
Set to Confirm?
1=YES   0=NO
```

This prompt pertains to the confirmation of RF and polling loop device serial numbers. When programming for the VistaKey, this entry can be used to confirm the DSMB serial number but is unnecessary.

Press either **1** or **0**. The following screen appears.

```
ENTER ZONE NO.?
000 = QUIT          010
```

Zone 010 entered ↑

Enter the 3-digit zone number for the VistaKey zone being programmed. As an example, 010 is shown here.

Press [✲] to accept the entry. The system advances to the summary prompt below.

When all zones (DSM, DSMB, RTE, and GP) have been programmed, enter **000** followed by [✲]. Then press **0** repeatedly until the "Access Point Pgm" prompt is displayed. Go to the "Setting Up Access Point Programming Options" paragraph is this section to program the access point(s).

```
010 ZT  P RC  B IN   L
    00  _ __  _ __  _
```

A display appears, showing a summary of that zone's programming. ZT = Zone Type, P = Partition, RC = Report Code, B = Bell/Aux Relay assignment for zone, IN = the input type of device, and L = the device's loop number to which the sensor is connected. Some devices can support more than one zone by means of individual loops. If the zone is not programmed, the display appears as shown here. If you are checking a zone's programming, and it is programmed satisfactorily, press [#] to back up one step and enter another zone number, if desired.

Otherwise, press [✲] to continue.

```
010 ZONE TYPE
```

Choose a response type for the DSM①, RTE②, General Purpose③, or DSMB① zone. Available zone types are listed below:

NOTE: The DSM, RTE, and General Purpose input zones should be only used for access control functions in UL installations.

00 = Assign for Unused Zones
01 = Entry/Exit #1, Burglary
02 = Entry/Exit #2, Burglary
03 = Perimeter, Burglary
04 = Interior Follower, Burglary
05 = Trouble Day/Alarm Night
06 = 24-Hr. Silent Alarm
07 = 24-Hr. Audible Alarm
08 = 24-Hr. Auxiliary
09 = Fire Without Verification④
10 = Interior Delay, Burglary
16 = Fire With Verification④
17 = Fire Waterflow④
18 = Fire Supervisory④
19 = 24-Hour Trouble
23 = No Alarm Response (e.g., relay activation)
29 = Momentary Exit⑤

① Zone type 01 or 02 is recommended for the typical DSM and DSMB zones to obtain an entry/exit delay. If a delay is not desired, zone type 03 is recommended.

② DO NOT assign a response type to the RTE zone when it is being used as a request to exit (controlling a door strike or mag lock). A response type may only be assigned when the RTE is NOT being used as a request to exit, which makes it an uncommitted zone. As an uncommitted zone, it may be assigned a response type for use as another type of zone.

③ In installations requiring supervision of the cabinet cover, the general purpose zone should be programmed as tamper (choose zone type 05).

④ These fire zones cannot be used in UL Installations.

⑤ Refer to "*Momentary Exit Access Points*" in this section for a complete description of Momentary Exit.

Press [*] to accept the entry and continue.

```
010   PARTITION
                  2
```

Enter the partition number you are assigning this zone to. The partition number assigned should be the same partition number as the one assigned to the protected area that the door (access point) is allowing entry to.

Press [*] to continue.

```
010 REPORT CODE
1st 03 2nd 12          3C
```

Enter the report code. The report code consists of 2 hexadecimal digits, each in turn consisting of 2 numerical digits. For example, for a report code of "3C," enter 03 for 3 and 12 for C.

NOTES:

- Entering 00 disables the reporting of all zone-related events. For a DSM input type, these are events like 423,46, 427, etc. and any report code that would normally be sent dictated by the zone type selection. (See *Event Log* section of this manual for a complete listing of ACS events). For a GP or uncommitted RTE zone, it disables reporting for all zone related events.

  Entering 00 overrides any ACS Dialer selections that may be enabled.
- If will be be using the ACS Report codes (ACS Dialer Events enabled), the zone report code must be set to a non-zero value.
- If ACS Dialer Events are being enabled, you must use the Contact ID reporting format.

(Refer to the *System Communication* section of your alarm system manual for more information about report codes and report code formats.)

Press [*] to continue.

010 BELL/RLY SEL
0

Each zone can be assigned to activate either one or both bell outputs and/or the system's auxiliary relay. Enter one of the following assignments:
0=none; 1=Bell 1; 2=Bell 2; 3=Bells 1 & 2; 4=Aux Relay; 5=Bell 1 & Aux Relay; 6=Bell 2 & Aux Relay; 7=Bells 1 & 2 & Aux Relay.
Press [*] to continue.

010 INPUT TYPE
RF Xmitter 3

Valid choices for this prompt, when programming the VistaKey, are Door Status Monitor (DSM), Request to Exit (RTE), General Purpose (GP), and serial number polling loop device (DSM Backup [DSMB]). The purpose of these input types are as follows:

DSM – This input type is used to map an access point to a zone. When the access point is bypassed, the controlled door is propped, or the controlled door is forced, the DSM operates according to the zone response type. The DSM device is normally a magnetic switch mounted on the door. The status of the switch is different while the door (access point) is in an open condition.

RTE – This input type is used to map an uncommitted RTE zone to an alarm panel zone. This input type is not normally used if the RTE zone is being used for a request to exit function. The RTE device may be something as simple as a momentary contact switch or as complex as a motion detector.

GP – This maps the GP zone to an alarm panel zone. This input type operates in the same manner as other VISTA 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 alarm panel. This zone is normally used for tamper in installations requiring supervision of the cabinet cover.

SERIAL POLL (DSMB) – The Serial Polling Loop input type (for DSMB) maps the SIM in the VistaKey to an Alarm Panel zone. In the event local power to the VistaKey is lost, the status of the DSM can no longer be reported to the panel via the normal micro-processor circuits of the VistaKey. In this case a Vplex SIM, which is located on the VistaKey board and powered directly from the polling loop, is activated and reports the state of the DSM via the standard Vplex polling system.

Enter the input device type as follows:

- 06 = serial number polling loop device (VistaKey DSM Backup Zone [VKey DSMB])
  NOTE: To obtain the DSMB function, this location (INPUT TYPE) must be defined as 06 and the next prompt (Access Point) must contain the Access Point # (01-15).
- 11 = VistaKey DSM Zone (VKey DSM)
- 12 = VistaKey RTE Zone (VKey RTE)
- 13 = VistaKey GP Zone(VKey GP)

Press [*] to continue.

If you pressed 11, 12, or 13, the system advances to the "Access Point" prompt. If you pressed 06, the system advances to the "Smart Contact" prompt or "V-Plex Relay" prompt.

```
010  Smart Contact
1 = YES  0 = NO      0
```

Press [**0**] and then press [✲] to continue.
NOTE: This prompt is not displayed on some alarm systems.

```
010  V-PLEX RELAY
1 = YES  0 = NO      0
```

Press [**0**] and then press [✲] to continue.

```
010  Access Point
(01-15)              3
```

Enter the 2-digit (01-15) door number for the VistaKey.

NOTE: The response to this question must be the address that was set in the VistaKey module for the door (access point) being programmed.

Press [✲] to continue.

If you entered an Input Type of 11, 12, or 13 above, the alarm system advances to the summary prompt. If you entered an Input Type of 06 and an access point number from 1 to 15 in the previous steps, the following "Input S/N:L" prompt appears for enrollment of the VistaKey serial number.

```
010  INPUT S/N:L
Axxx-xxxx:1
```

To enroll the VistaKey (DSMB) serial number:

1. Remove power from the VistaKey module.
2. Activate the DSM Zone until the keypad beeps twice and the VistaKey serial number is displayed.
3. Remove the fault from the DSM Zone and re-apply power to the VistaKey.

NOTE: When you enroll the VistaKey DSMB zone, you assign it to loop 1; loop 2 must be unused.

Press [✲] to continue.

```
010 ZT  P RC  B IN   L
    01  2 3C  0 DM  1
```

The summary screen for the zone appears.

NOTE: The input type for the device (IN) portion of the display is dependent on the choice made at the INPUT TYPE prompt above; it is either RE (type 12 – Request to Exit), GP (type 13 – General Purpose), or DB (type 06 – Door Status Monitor Backup).

Press [✲] to accept the zone information.

The alarm system control will return to the "ENTER ZONE NO." prompt.

Setting Up Access Point Programming Options for Each VistaKey Module

Access point options for the VistaKey module(s) are set using Access Point Programming. To reach Access Point Programming, enter **#93 Menu Mode Programming** and press the [**0**] key until the following prompt is displayed.

```
Access Point Pgm
1=Yes   0=No
```

Press **1** or **0** to select Access Point Programming or to bypass Access Point Programming.

If you press 1, the keypad displays the following prompt.

If you press 0, the keypad advances to Access Group Programming.

```
ENTER ACS PT#
01-15, 00=Quit      01
```

Enter a number from **01** to **15** for the access point number to be programmed; or **00** to Quit Access Point Programming. The number entered here for the access point number is the setting of the VistaKey address switch (1 through 9 = 01 through 09, A=10, B=11, C=12, D=13, E=14, or F=15).

Press [✲] to accept the entry.

If you have finished programming the access points, enter **00**. The alarm control panel advances to Access Group Programming.

If you enter a number from 01 through 15, the keypad displays the following prompt.

```
↓ Access Point Number
01 DSM CONFIG
NORM OPEN           0
```

Enter 1 digit for the DSM zone (VistaKey zone A) configuration. The configuration entered must be the DSM status when the door (access point) is closed. Acceptable 1-digit entries are as follows:

0 = normally open
1 = normally closed
2 = EOLR normally open
3 = EOLR normally closed

Press **[✲]** to accept the entry.

```
↓ Access Point Number
01 DOOR OPN TIME
3s                  2
```

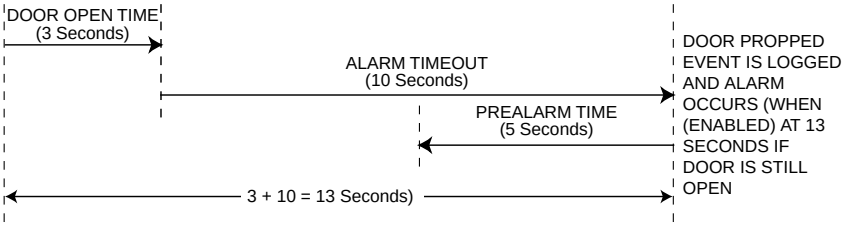
The door open time is the amount of time that the door-locking device is kept in the unlocked (open) status following a valid card swipe at the card reader or RTE (if enabled), unless a relatch condition occurs. Enter 1 digit (0 to 7) for the door strike relay duration in seconds.

0 = 1 second	4 = 5 seconds
1 = 2 seconds	5 = 10 seconds
2 = 3 seconds	6 = 15 seconds
3 = 4 seconds	7 = 30 seconds

Press **[✲]** to accept the entry.

```
↓ Access Point Number
01 ALARM TIMEOUT
10s                 0
```

Enter 1 digit for the door alarm timeout value. The timer for alarm timeout starts at the end of the door open time defined above; therefore, the total amount of time before a zone fault is issued is the amount set for the door open time plus the amount of time entered for this prompt (see figure below). If the access point is still open when the timeout value entered has expired, a zone fault (alarm timeout) is reported to the VISTA panel and a Door Propped event is logged.



Acceptable 1-digit entries are as follows:

0 = 10 sec.	4 = 2 min.
1 = 20 sec.	5 = 5 min.
2 = 30 sec.	6 = 10 min.
3 = 1 min.	7 = 30 min.

Press **[*]** to accept the entry.

↓ Access Point Number

01 PREALARM TIME	
5s	0

The pre-alarm time is used to warn a person holding the access door open that a zone fault (resulting in an alarm when enabled) will occur if the door is not closed before the alarm timeout expires. (For example, as shown in the above figure, if the alarm timeout is set for 10 seconds and the pre-alarm time is 5 seconds, the pre-alarm warning commences 5 seconds before the alarm condition [zone fault] is reported to the VISTA panel.) The pre-alarm signal is output from the VistaKey on the Trigger output and if used, must be enabled when responding to the PREALARM TRIG prompt later in this section.

Enter 1 digit for the door pre-alarm timeout value. Acceptable 1-digit entries are as follows:

0 = 5 sec.	4 = 1 min.
1 = 10 sec.	5 = 2 min.
2 = 15 sec.	6 = 5 min.
3 = 30 sec.	7 = 10 min.

Press **[*]** to accept the entry.

↓ Access Point Number

01 RELATCH on	
timeout/closed	0

When a DSM zone is installed at the door, the system can determine that the door has closed before the amount of time that it was to remain unlatched (see “Door Opn Time” prompt above). When the “relatch on timeout/closed” option is selected, the system automatically relatches the door when it closes or at timeout, whichever occurs first. The “timeout/closed” option prevents a late-comer from pushing an unlatched door open. When “relatch on open” is selected, the door strike or mag lock will relatch as soon as the door is opened.

Press **0** (relatch on timeout or door closing, whichever occurs first) or **1** (relatch on door opening).

Press **[*]** to accept the entry.

↓ Access Point Number

```
01 RTE CONFIG
NORM OPEN        0
```

Enter 1 digit for the uncommitted RTE zone (VistaKey zone B) configuration. The choice entered for this selection must be the status of the RTE device (switch) when it is not active (in the ready state). Acceptable 1-digit entries are as follows:

0 = normally open
1 = normally closed
2 = EOLR normally open
3 = EOLR normally closed

Press **[*]** to accept the entry.

↓ Access Point Number

```
01 RTE RETRIGGER
NOT ENABLED      0
```

This prompt is used to extend the time the door may remain open without an alarm when the door is already in an open condition. When enabled, each additional Request to Exit (RTE) restarts the alarm timeout defined in the "ALARM TIMEOUT" prompt above. This selection allows a line of people to exit without an alarm being issued because of the amount of time the door is open.

NOTE: RTE Retrigger is only applicable if the RTE function (VistaKey Zone B) is enabled in the below prompt. If VistaKey Zone B is being used as an uncommitted zone, the response to this prompt will not have any effect on system operation.

Press **1** if additional RTEs are to restart the alarm timeout. Press **0** if the additional RTEs should not restart the alarm timeout.

↓ Access Point Number

```
01 RTE ENABLED?
ENABLED          1
```

This prompt is used to define if the RTE is to be enabled (committed/used for the access point) or not enabled (uncommitted/not used for the access point). Enabling the RTE allows the VistaKey to request and/or grant an access via this zone input. Disabling the RTE causes this zone to be an uncommitted zone; i.e., the VistaKey will not be able to grant access via this zone.

NOTE: Remember that uncommitted means that VistaKey zone B is not being used for a RTE function and it then may be used in the same manner as any other zone.

Press **1** to select if the RTE is to be enabled. Press **0** to disable the RTE.

↓ Access Point Number

```
01 RTE DOORSTRIKE
ENABLED          1
```

This prompt is used to define whether the RTE (if enabled in the previous step) will unlock the doorstrike and start the exit timeouts (1) or just start the exit timeouts (0). This option is normally set to 1. This option may be set to 0 if the door can be unlatched from the inside manually (i.e., working doorknob).

NOTE: RTE Doorstrike is only applicable if the RTE function (VistaKey Zone B) is enabled in the above prompt. If VistaKey Zone B is being used as an uncommitted zone, the response to this prompt will not have any effect on system operation.

Press **0** to prevent the RTE from unlocking the doorstrike.
Press **1** to cause the RTE to unlock the doorstrike.

↓ Access Point Number

01 GP CONFIG	
NORM OPEN	0

Enter 1 digit for the general purpose zone (VistaKey zone C) configuration. This zone is normally used for a tamper when the VistaKey cabinet requires supervision. Acceptable 1-digit entries are as follows:

0 = normally open
1 = normally closed
2 = EOLR normally open
3 = EOLR normally closed

Press **[*]** to accept the entry.

↓ Access Point Number

01 PREALARM TRIG	
NOT ENABLED	0

The prealarm trigger prompt is used to define if the prealarm trigger is to be enabled. If the prealarm trigger is enabled, the trigger will be activated when the prealarm time begins (see PREALARM TIME and ALARM TIMEOUT prompts above) and be deactivated when the access point closes. This output can be used for a door propped alarm.

Press **1** to enable the prealarm trigger output.
Press **0** to disable the prealarm trigger and make the trigger output uncommitted.

↓ Access Point Number

01 TRIG MODE	
NOT USED	0

The mode of operation of the trigger can be set to "discrete," "one-shot," or "repeating." A discrete trigger will become energized when commanded on and will stay energized until commanded off. An example of a discrete trigger is when a door is open and a timeout occurs (door fault), the trigger turns on and it remains on until the door is closed (fault removed). A one-shot trigger energizes once when commanded on, stays on for the specified on time, then shuts off. A repeating trigger output cycles on and off for the specified amount of on time, off time, and for the specified number of repeat counts. If the repeat count is set to zero, the cycling continues until the trigger is commanded off.

Press **0** through **3** for the trigger action mode.

0 = not used (If you select 0, the system advances to the ACCESS GROUP prompt below.)
1 = discrete (If you select 1, the system advances to the ACCESS GROUP prompt below.)
2 = one-shot (If you select 2, the system advances to the "TRIG ON TIME" prompt.)
3 = repeating (If you select 3, the system advances to the "TRIG REPT CNT" prompt below.)

Press **[*]** to accept the entry.

↓ Access Point Number

01 TRIG RPT CNT	
Continuous	0

Enter 1 digit representing the number of repeated on/off cycles that are output by the trigger function. If this number is set to 0, the trigger repeats continuously until it is commanded off. Acceptable 1-digit entries are as follows:

0 = continuous	4 = 4 cycles
1 = 1 cycle	5 = 5 cycles
2 = 2 cycles	6 = 10 cycles
3 = 3 cycles	7 = 25 cycles

Press **[*]** to accept the entry.

↓ Access Point Number

```
01TRIG OFF TIME
1s                0
```

Enter 1 digit for the time, in seconds, that the trigger is to remain de-energized if its mode is set as repeating. This is the time that makes up the "OFF" time of a repeating cycle. Acceptable 1-digit entries are as follows:

0 = 1 sec.	4 = 5 sec.
1 = 2 sec.	5 = 10 sec.
2 = 3 sec.	6 = 15 sec.
3 = 4 sec.	7 = 30 sec.

Press **[*]** to accept the entry.

```
01 TRIG ON TIME
1s                0
```

Enter 1 digit for the time, in seconds, that the trigger is to remain energized if its mode is set as one-shot. If the mode is set as repeating, this is the time that makes up the "ON" time of a repeating cycle. Acceptable 1-digit entries are as follows:

0 = 1 sec.	4 = 10 sec.
1 = 2 sec.	5 = 30 sec.
2 = 3 sec.	6 = 1 min.
3 = 5 sec.	7 = 2 min.

Press **[*]** to accept the entry.

```
ACS GRP?1 2 3 4 5 6 7 8
HIT 0-8   x x x x x x x x
```

Select the access groups that will be allowed entry or egress through this access point when their respective access group is enabled via scheduling. Note that cardholders with executive privileges enabled have access to all access points regardless of this setting. Also note that cardholders with expired cards will not have access to any access point, regardless of this setting.

Press **0** to toggle all access groups on or off; or press keys **1**-**8** to toggle the letter "x" under the access group numbers on or off.

Press **[*]** to accept the entry.

```
RDR CONFIG
WEIGAND           0
```

This prompt accepts 0 (Weigand) or 1 (Clock/Data). The ADEMCO reader is a Weigand configuration (format) reader.

Press **0** for a Weigand reader configuration.

Press **[*]** to accept the entry.

↓ Access Point Number

```
01 RDR POSITION
Entry             0
```

Enter the reader position as either ENTRY or EXIT. This is important for EXIT EVENT and ENTRY EVENT event/action selection during Access Group Programming and determines how associated events are logged and reported (e.g., Access Grant, Egress Grant).

Press **0** or **1** to select if the reader is an entry reader (0) or an exit reader (1).

Press **[*]** to accept the entry.

The system will return to the "ENTER ACS PT#" prompt.

Setting Up Access Groups

Access groups for the VistaKey are set using Access Group Programming. To reach access group programming, enter **#93 Menu Mode Programming** and press the [**0**] key until the following prompt is displayed.

```
ACCESS GRP PGM
1=YES   0=NO        0
```

Press **1** or **0**.

If you press 1, the keypad displays the following prompt.

When you have completed Access Group Programming, press **0**; the alarm panel control advances to Event/Action Programming.

Note that when assigning cards to a new access group, the cards in the new access group will not be functional until the new access group is enabled (via #77, time schedules, etc.).

```
ACCESS GROUP
01-08, 00=QUIT      01
```

Enter a number from **01** to **08** for the group number to be programmed, or **00** to quit Access Group Programming.

Each cardholder must belong to at least 1 access group. The access group provides the cardholder with certain privileges afforded to all cardholders that belong to that access group. If a cardholder belongs to more than 1 access group, he is afforded all the privileges of all the access groups he belongs to. The access groups determine which access point(s) the cardholder has access to and at what times according to the schedule by which his access group is enabled.

Press **[*]** to accept the entry.

If you entered a number from 01 through 08, the keypad displays the following prompt.

When you have completed all Access Group Programming, enter **00**; The alarm system control advances to Event Action Programming.

↓ Access Group Number

```
01 EXEC PRIV?
NOT ENABLED         0
```

Press **1** (enable) or **0** (disable) to define whether the group has executive privileges.

Enabling Executive Privilege enables all cardholders in this group to access any access point and disarm the access point's partition (if armed) at any time regardless of whether the cardholder's access group is enabled via scheduling or whether his access group is enabled to enter or exit through any of the access points. The only reason that a cardholder with executive privilege would be prevented from gaining access through an access point is if his card has expired via usage or date. Disabling executive privilege allows cardholders entry through access points only if the access point has been programmed to accept the cardholder's access group (see *Access Point Programming* section); the cardholder's access group is enabled at the time of the card swipe (via scheduling, event/action or action selector), PIN entry (code+#73), or RF button remote depression; AND the cardholders card has not expired.

NOTE: Executive privilege for an access group will not have any effect when a VistaKey module is operating in Reduced Capability Mode (RCM). Only executive privilege assigned to a cardholder will provide all of the executive privileges described during RCM.

Press **[*]** to accept the entry.

↓ Access Group Number

```
01 Trace?
NOT ENABLED      0
```

Press **1** (trace) or **0** (no trace) to define whether the cardholders in the group are to be traced.

Enabling the trace feature allows this access group to be monitored by logging entry/exit grants and denials in the alarm panel log and/or dialing out and sending a report to the central station.

Press **[*]** to accept the entry.

↓ Access Group Number

```
01 Restr?1 2 3 4 5 6 7 8
HIT 0-8
```

Press **0** to toggle Armed Restriction for all VISTA partitions on or off; or press keys **1**-**8** (VISTA-128FB) or 1-2 (VISTA-32FB) to toggle the letter "x" under the Armed Restriction partition numbers on or off.

NOTE: When the Armed Restriction is enabled for a partition and the partition is armed, a cardholder will be denied access through access points in a partition when both of the following conditions exist:

1. All access groups that the cardholder belongs to have an Armed Restriction for the partition and none have executive privilege.
2. The cardholder's VISTA User # does not have access permission for the partition.

Press **[*]** to accept the entry.

↓ Access Group Number

```
01 Entry Event?
Never Invoke     00
```

Enter two digits from the following list for the access point-related entry event that causes the entry action desired. Acceptable entries and their meanings are as follows:

00 Never Invoke - causes no action to take place on entry.
02 Access Request (Acs Req) - causes the ENTRY ACTION to occur when a card swipe occurs on an entry card reader.
04 Any Request (Any Req) - causes the ENTRY ACTION to occur when a card swipe occurs on an entry or exit card reader.
05 Access Grant (Acs Grt) - causes the ENTRY ACTION to occur when an access grant occurs on an entry card reader.
07 Any Grant (Any Grt) - causes the ENTRY ACTION to occur when any grant occurs on an entry card reader.
08 Access Denied (Acs Deny) - causes the ENTRY ACTION to occur when an access denied occurs on an entry card reader.
10 Any Denial (Any Deny) - causes the ENTRY ACTION to occur when any denial occurs on an entry card reader.

NOTE: The entry event selected only applies when the card swiped belongs a member of the access group currently being defined and the swipe occurs at the access point defined in the following prompt.

Press **[*]** to accept the entry.

↓ Access Group Number

```
01 Access Point
(01-15)          01
```

Enter 1 through 15 for the access point number corresponding to the entry event defined above.

Press **[*]** to accept the entry.

↓ Access Group Number

01 Entry Action?	
None	00

Enter two digits defining the entry action desired. For acceptable entries and their meanings, see *Table 5-1: Action Codes*; or enter 00 for no action. The following rules apply to the selected entry action:

- The action only occurs when the above entry event occurs at the access point selected and the card triggering the event is assigned to this access group.
- Actions that arm or disarm partitions are only performed if the VISTA user assigned to the card is assigned to the partitions selected.

NOTE: When you use action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only), these actions disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.

Press **[*]** to accept the entry.

In response to the entry action you entered, the system displays a message asking for additional information, based on the entry action you selected. For example, if the entry action you selected was **01** (relay on), the system presents a message asking for a relay number. Respond to the message and then press **[*]** to accept the entry.

↓ Access Group Number

01 Exit Event?	
Never Invoke	00

Enter 00 through 10 for the access point-related exit event desired. Acceptable entries and their meanings are as follows:

00 Never Invoke - causes no action to take place on exit.
03 Egress Request (Egr Req) - causes the EXIT ACTION to occur when a card swipe occurs on an exit card reader.
04 Any Request (Any Req) - causes the EXIT ACTION to occur when a card swipe occurs on an exit or exit card reader.
06 Egress Grant (Egr Grt) - causes the EXIT ACTION to occur when an access grant occurs on an exit card reader.
07 Any Grant (Any Grt) - causes the EXIT ACTION to occur when any grant occurs on an exit card reader.
09 Egress Denied (Egr Deny) - causes the EXIT ACTION to occur when an egress denied occurs on an exit card reader.
10 Any Denial (Any Deny) - causes the EXIT ACTION to occur when any denial occurs on an exit card reader.

NOTE: The exit event selected only applies when the card swiped belongs a member of the access group currently being defined and the swipe occurs at the access point defined in the following prompt.

Press **[*]** to accept the entry.

↓ Access Group Number

01 Access Point	
(01-15)	01

Enter 1 through 15 for the access point number corresponding to the exit event defined above.

Press **[*]** to accept the entry.

↓ Access Group Number

01 Exit Action?	
None	00

Enter two digits defining the exit action desired. For acceptable entries and their meanings, see *Table 5-1: Action Codes* earlier in this section, or enter 00 for no action. The following rules apply to the selected exit action:

- The action only occurs when the above exit event occurs at the access point selected and the card triggering the event is assigned to this access group.
- Actions that arm or disarm partitions are only performed if the VISTA user assigned to the card is assigned to the partitions selected.

NOTE: When you use action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only), these actions disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.

Press **[*]** to accept the entry.

In response to the exit action entered, the system displays a message asking for additional information, based on the exit action you selected. For example, if the exit action selected was **01** (relay on), the system presents a message asking for a relay number. Respond to the message and then press **[*]** to accept the entry.

The program returns to the "Access Group" prompt so that another access group may be programmed.

NOTES:

- Users will be assigned to the access group(s) later using the *Performing Access Control Card Functions* procedures in *Section 6: User Commands*.
- Newly defined access groups must be enabled before they become active. This enable is performed after leaving #93 Menu Mode Programming and is described under *Enabling Access Groups* later in this section.

Programming Event/Actions

Event/Actions are used to make something occur (action) when something happens (event). One example is turning on a light (via a relay) when anyone is allowed to enter (access grant).

Event/Actions for the VistaKey are set using Event/Action Programming. To reach event/action programming, enter **#93 Menu Mode Programming** and press the [**0**] key until the following prompt is displayed.

```
EVENT/ACTION PGM
1=YES  0=NO        0
```

Press **1** or **0**.

If you press 1, the keypad displays the following prompt.

NOTE: Before you enter Event Action Programming, complete the procedures and worksheet provided in *Preparing an Event/Action Worksheet* in this section. The responses should come from your worksheet.

If you press 0, the alarm system control advances to the Quit Menu Mode programming prompt.

```
Event/Action#
(01-32), 00=quit   01
```

Enter a number from **01** to **32**, from your Event/Actions Worksheet, that corresponds to the event/action to be programmed; or **00** to quit Event/Action Programming.

Press **[*]** to accept the entry.

If you enter a number from 01 through 32, the keypad displays the following prompt.

If you enter 00, the alarm system control advances to Quit Programming.

↓ Event/Action Number

```
01 Acs Event?
None                00
```

Enter two digits defining the number for the event from the Event No. column of your worksheet. The entry falls into 1 of 6 different categories. Acceptable entries are as follows:

Partition Specifiers

No.	Description	No.	Description
00	None (Not Used)	09	Duress Ptn
01	Arm Ptn	10	Duress Restore Ptn
02	Disarm Ptn	11	Trouble Ptn
03	Fire Ptn	12	Trouble Restore Ptn
04	Fire Restore Ptn	13	Bypass Ptn
05	Burg Ptn	14	Bypass Restore Ptn
06	Burg Restore Ptn	15	Late Disarm Ptn
07	Alarm Ptn	16	Early Arm Ptn
08	Alarm Restore Ptn	17	Fail Arm Ptn

User Specifiers

No.	Description	No.	Description
18	Arm User	20	Grant User
19	Disarm User		

Card ID Specifiers

No.	Description
21	Grant Card

Access Point (AP) Specifiers

No.	Description	No.	Description
22	AP Grant	30	Duress Grant
23	AP Deny	31	Prop Open Alarm
24	AP Bypass	32	Prop Open Restore
26	AP Lock	33	Force Open
27	AP Protect	34	Force Open Restore
29	AP Grant Override		

Zone Number Specifiers

No.	Description	No.	Description
35	Fire Zone	40	Alarm Restore Zone
36	Fire Restore Zone	41	Trouble Zone
37	Burg Zone	42	Trouble Restore Zone
38	Burg Restore Zone	43	Bypass Zone
39	Alarm Zone	44	Bypass Restore Zone

Arming Specifiers

No.	Description	No.	Description
45	Arm Stay Ptn	49	Arm Stay User
46	Arm Away Ptn	50	Arm Away User
47	Arm Instant Ptn	51	Arm Instant User
48	Arm Maximum Ptn	52	Arm Maximum User

Press **[*]** to accept the entry.

In response to the number for the event that was entered, the system displays a message asking for additional information based on the entry definition. For example, if the entry was **01** (arm partition), the system presents a message asking for a partition number. Respond to the message and then press **[*]** to accept the entry.

↓ Event/Action Number

```
01 ACTION?
None                00
```

Enter the Action Number listed in your worksheet. This is the action that will occur when the event occurs within the time window and days selected.

Press **[*]** to accept the entry.

In response to the action entered, the system displays a message asking for additional information based on the action selected. Respond to the message and then press **[*]** to accept the entry.

↓ Event/Action Number

```
01 Time Window ?
Always Active       00
```

Enter the 2-digit time window entry from your worksheet (00 = always active, 01-20 = time window #). This is the time window in which the action will occur. If always active (00), then the action will occur any time the event occurs. Otherwise, the event must occur within this time window and day selected for the action to occur.

Press **[*]** to accept the entry.

```
DAYS ?   MTWTFSSH
HIT 0-8
```

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).

NOTE: When holiday is selected, it will over-ride the day of the week selection (e.g., Holiday is selected and the holiday falls on Saturday but Saturday is not selected, the Holiday selection makes the Event/Action active).

Press **[*]** to accept the entry.

The system returns to the "Event/Action#" prompt for programming additional event/actions.

Quit #93 Menu Mode Programming

```
QUIT MENU MODE?
1=Yes  0=No         0
```

Press **1** to quit or **0** to return to the "ZONE PROG.?" prompt.

Programming Time-Driven Events

Time-driven events are used to make something occur (action) based on time. Time-driven events are programmed via the Alarm Panel #80 Scheduling Menu Mode. To program time-driven events, perform the procedures provided in "Preparing a Time-Driven Events Worksheet" provided earlier in this section; and then, using the procedures provided in your alarm system Installation and Setup Guide:

1. Define any new time windows that are used by your time-driven events.
2. Enter the information from your Time-Driven Events Worksheet located near the end of this section.

Enabling Access Groups

When an access group is entered into the system for the first time, the group must be enabled. The access group can be enabled either by time-driven events or by the #77 command. If you are using time-driven events, the Time-Driven Events Worksheet (see *"Preparing a Time-Driven Event Worksheet"* in this section) and the *"Programming Time-Driven Events"* above must be completed to enable the access group if you have not already done so. If you are using the other method (#77) to enable the access group, proceed as follows:

1. Enter **Installer Code** + **#77**.
2. Enter action number 77 (to enable access groups).
3. Enter the access group number.
4. Quit.

Additional System Considerations

The following paragraphs contain information about features that may be used to customize the operation of the VistaKey/alarm panel as well as installation and programming considerations.

Momentary Exit Access Points

The system contains a feature that allows an entry reader to be momentarily (15 seconds) turned into an exit reader. This feature allows the user or access group to perform such tasks as arming the alarm system by swiping a card while exiting the building. To utilize this feature, a switch must be wired to an available zone and the system must be programmed to activate the momentary exit function. To install this feature, observe the following procedure:

1. Connect a switch to an available zone. Configure the connection so that when the switch is activated, the zone is shorted. Either mount this switch so that it is not readily accessible to all people entering or leaving the building, or use a key-switch.
2. To program the VISTA Alarm Panel for the Momentary Exit function, enter #**93 Menu Mode Programming** in the alarm system in accordance with the procedures provided in your alarm system manuals. The following message is displayed on the keypad:

ZONE PROG? 1=YES 0=NO

Press **1** to enter Zone Programming. The following screen appears.

NOTE: During programming, press [✲] to display the next screen. Press [**#**] to display a previous screen.

Set to Confirm? 1=YES 0=NO

This prompt pertains to the confirmation of RF and polling loop device serial numbers. When you are programming for the Momentary Exit function, the response to this entry does not affect programming. Press either **1** or **0**. The following screen appears.

ENTER ZONE NO.? 000 = QUIT 008

Zone 008 entered ↑

Enter the 3-digit zone number for the VistaKey zone being programmed. As an example, 008 is shown here.

Press [✲] to accept the entry. The system advances to the summary prompt below.

008 ZT P RC B IN L 00 _ __ _ __ _	A display appears showing a summary of that zone's programming. ZT = Zone Type, P = Partition, RC = Report Code, B = Bell/Aux Relay assignment for zone, IN = the input type of device, and L = the device's loop number to which the sensor is connected. Some devices can support more than one zone by means of individual loops. If the zone is not programmed, the display appears as shown here. Press [*] to continue.
008 ZONE TYPE	Press **29** for momentary exit. Press [*] to accept the entry and continue.
008 Access Point (01-15) 3	Enter the 2-digit (01-15) door number for the VistaKey. **NOTE:** The response to this question must be the address that was set in the VistaKey module for the door (access point) being programmed. Press [*] to continue.
008 Entry or Exit Entry 0	Always press **1** for Exit. Note that this is a standard message display used for programming access points and that you should never respond with 0 (entry) when defining a momentary exit zone. Press [*] to continue.
008 PARTITION 2	Enter the partition number that the access point is assigned to. Press [*] to continue.
008 REPORT CODE 1st 03 2nd 12 3C	When you are programming for the Momentary Exit function, the response to this entry does not affect operation. Press [*] repeatedly until the INPUT TYPE prompt appears.
008 INPUT TYPE Hardwire 01	Enter the zone input type. In this example, zone 8 is a hardwired zone. Press [*] to continue.
008 ZT P RC IN L 29 2 80 HW 1	The summary screen for the zone appears. Press to accept the zone information. The alarm system control returns to the "ENTER ZONE NO." prompt. Enter "000" and then press [*] to exit Zone Programming.

3. Exit #93 Menu Mode Programming.
4. The action to be performed on exit can be assigned to either an access group or a cardholder. To assign the action on exit to an access group, observe the items listed under **a.** below. To assign the action on exit to a cardholder, observe the items listed under **b.** below.
   a. To assign the action on exit to an access group, use the procedures provided in "Setting Up Access Groups" described earlier in this section. When setting up access groups, observe the following:

- At the "Exit Event?" prompt, enter 06 for Egress Grant.
- At the "Access Point?" prompt, specify the access point at which the Egress Grant must take place.
- At the "Exit Action?" prompt, enter the code for the desired exit action (i.e., 21 for Arm-Away). A listing of the Action Codes is provided in *Table 5-1: Action Codes*. The following rules apply to the selected exit action:

  The action only occurs when the above exit event occurs at the access point selected and the card triggering the event is assigned to the access group being programmed.

  Actions that arm or disarm partitions are only performed if the VISTA user assigned to the card is assigned to the partitions selected.

  Actions that grant access to access points will only be performed if the card has access to these access points.

  Actions that change the state (bypass, lock, protect, exit only) of access points are only performed if the VISTA user assigned to the card is assigned to the partition to which the access points are assigned.

b. To assign the action on exit to a cardholder, use the procedures provided in "Performing Access Control Card Functions" described later in *Section 6: User Commands*. When setting up the cardholder, observe the following:

- At the "ACS Event?" prompt, enter 06 for Egress Grant.
- At the "Access Point?" prompt, specify the access point at which the Egress Grant must take place.
- At the "Action?" prompt, enter the code for the desired exit action (i.e., 21 for arm-Away). A listing of the Action Codes is provided in *Table 5-1: Action Codes*. If the action selection requires a partition or other specifier, a prompt requests the partition or other specifier. The following rules apply to the selected exit action:

  Actions that arm or disarm partitions are only performed if the VISTA user assigned to the card is assigned to the partitions selected.

  Actions that grant access to access points will only be performed if the card has access to these access points.

  Actions that change the state (bypass, lock, protect, exit only) of access points are only performed if the VISTA user assigned to the card is assigned to the partition to which the access points are assigned.

The system has been set up for the Momentary Exit function, which performs the action you specified when the group or cardholder exits. To use the function, the access group member or cardholder energizes the switch. In response, the reader at the access point becomes an exit reader for 15 seconds, during which time a card swipe causes the exit action to take place.

Access 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 for the following event categories:

- ACS Troubles
- ACS Bypasses
- ACS System (i.e., ACS module reset, entry/exit test)
- ACS Alarms

- ACS Trace (To obtain a report for Trace, the ACS Group Trace or Cardholder Trace must also be turned on.)

NOTE: See *Section 8: Event Log* for a listing of the events and report codes that make up each of these categories.

The system contains provisions that allow you to change the program defaults so that reports are sent for any or all of these event categories. To change the defaults in the program, enter the **Data Field Program Mode** using the procedures in your alarm system manuals. The keypad displays:

Program Mode * Fill # View –00	Press ✳**94**. The following screen appears.
Program Mode * Fill # View 100	Press ✳**35**. The following screen appears.
ACS Dlr Enables 135	This field requires the entry of 6 digits. The entries for this field are as follows:

ENTRY ORDER	EVENT	ENTRY
1	ACS Trace	Always press **1** if reports are to be sent for Trace. Press **0** only if no reports are to be sent.
2	ACS TROUBLES	Press **1** to enable or **0** to disable ACS trouble reporting.
3	ACS BYPASSES	Press **1** to enable or **0** to disable ACS bypass reporting.
4	Reserved	Press **1** or **0**. This entry is required as a placeholder in the six-digit string.
5	ACS SYSTEM	Press **1** to enable or **0** to disable ACS system reporting.
6	ACS ALARMS	Press **1** to enable or **0** to disable ACS alarm reporting.

The keypad beeps three times after you enter the sixth digit.

Press [✳]. The following screen appears.

Enter Fill Field 1	Press **#99**. The following screen appears.
Program Mode * Fill # View –00	Press **#99** again. The Data Field Programming Mode ends.

#73 Keypad Entry Enable

The #73 command may be used (if enabled) to grant entry or exit through an access point in the partition that the keypad is connected to. The access point automatically relatches after the time interval set by the previously defined door open time. For the #73 command to be accepted, the following conditions must exist.

- The keypad must be attached to the partition where the access point is located.
- If the partition is armed and Armed Restriction is in effect, the user must be authorized to disarm the partition.

- The user must be assigned to the partition. If not the user will not be accepted at the keypad.
- The user must be assigned to a card that has access to the point specified.
- The user must have access to the partition at the time the command is entered.

To enable this feature, enter #**93 Menu Mode Programming** in the alarm system in accordance with the procedures provided in your alarm system manuals. The following message is displayed on the keypad:

ZONE PROG? 1=YES 0=NO	Press **1** to enter Zone Programming. The following screen appears. **NOTE:** During programming, press [✳] to display the next screen. Press [**#**] to display a previous screen.
Set to Confirm? 1=YES 0=NO	This prompt pertains to the confirmation of RF and polling loop device serial numbers. When you are programming for the #73 function, the response to this entry does not affect programming. Press either **1** or **0**. The following screen appears.
ENTER ZONE NO.? 000 = QUIT 025 Zone 025 entered ↑	Enter the 3-digit zone number for the zone being programmed to accept an access point command. As an example, 025 is being shown here. Press [✳] to accept the entry. The system advances to the summary prompt below.
025 ZT P RC B IN L 00 _ __ _ __ _	A display appears showing a summary of that zone's programming. ZT = Zone Type, P = Partition, RC = Report Code, B = Bell/Aux Relay assignment for zone, IN = the input type of device, and L = the device's loop number to which the sensor is connected. Some devices can support more than one zone by means of individual loops. If the zone is not programmed, the display will appear as shown here. Press [✳] to continue.
025 ZONE TYPE	Press **27** for access point. Press [✳] to accept the entry and continue.
025 Access Point (01-31) 00	Enter the 2-digit (01-15) door number for the VistaKey: **NOTE:** The response to this question must be the address that was set in the VistaKey module for the door (access point) being programmed. Press [✳] to continue.
025 Entry or Exit Entry 0	Press **0** for Entry or **1** for Exit. The selection entered should match (entry or exit) the access point being accessed. Note that this affects the event that gets logged and reported so, you want to select entry for an entry point and exit for an exit point. Press [✳] to continue.
025 PARTITION 1	Enter the partition number that the access point is assigned to. Press [✳] to continue.

025 REPORT CODE 1st 01 2nd 00 10	When you are programming for the #73 function, the response to this entry does not affect operation. Press [✲] repeatedly until the "INPUT TYPE" prompt appears.
025 INPUT TYPE None 00	Enter the zone input type as **09** for Console. Press [✲] to continue.
025 Cons ECP Addr (00-30) 00	Enter the 2-digit ECP address of the keypad. Press [✲] to continue.
025 ZT P RC IN L 27 1 10 CS 1	The summary screen for the zone appears. Press [✲] to accept the zone information. The alarm system control returns to the "ENTER ZONE NO." prompt. Enter "000" and then press [✲] to exit Zone Programming. Exit #93 Menu Mode Programming.

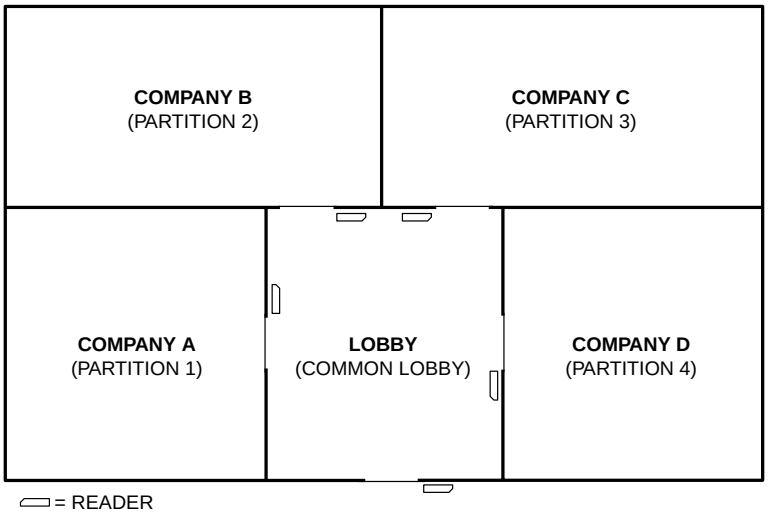
The system has been set up for the #73 command to unlatch the access point programmed when the command is issued by a valid user at the keypad.

Alarm System Levels of Authority

When you are installing a VistaKey in an alarm system, it is important to review the levels of authority assigned to the users of the system. The Installer Level (Authority Level 0) and the Master Level (Authority Level 1) can:

- Enroll cards into the system
- Issue all action commands listed in *Table 5-1: Action Codes*

For example, if the building contains four companies (see diagram below) and each company has a Master Level user assigned, that user can assign cards for other companies and/or control their access points by issuing action commands. Because of this, the highest level assigned to any company should be Manager (Authority Level 2); the Master Level should only be assigned to the user responsible for security in the whole building.



Removing a VistaKey

A VistaKey can be removed (deleted) from the alarm system database. To delete a VistaKey, proceed as follows:

1. Enter zone programming.
2. Advance to the zone numbers that the VistaKey DSM, DSMB, RTE, and General Purpose zones are assigned to.
3. Set the Zone Input type to “None” or set the Zone Response type to “None” and answer “Yes” to the “Delete Zone?” query. This removes all definitions for the zone.

Time-Driven Events Worksheet

Timed Event #	Action No.	Action Name	Action Specifier	Time Window	Activation Time	Days							
						M	T	W	T	F	S	S	H
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													

Event/Actions Worksheet

Event	Event No.	Event Name	Event Specifier	Action No.	Action Desired	Action Specifier	Time Window (00= Always, 01-20 = Time Window #)	Days							
								M	T	W	T	F	S	S	H
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															

SECTION 6

User Commands

In This Section

General Information

When the VistaKey is attached to the alarm system, the alarm panel user has additional commands and may have the ability to control the access card database. This section contains the additional user commands and instructions for performing access control card management functions.

Additional User Commands

The following commands are used to control access points, test the access system, and/or control cardholders:

Command Type	Command	Description
Access Control	User Code + # + 73	Request to enter/exit (accepted for User's authorized partition only)
	User Code + # + 74 + Access Point Number + Entry or Exit	Request to enter/exit at access point (accepted for User's authorized partition only)
	User Code + # + 75 + Access Point Number + Door Command	Change access point state - activate grant/protect/bypass (accepted for user's authorized partition only)
	User Code + # + 79	Perform access control card functions
Output Device Control	User Code + # + 77	Activate any action
Access Control Test	User Code + # + 78 + Grant Command	Perform access control test using database cards or all cards
Schedule Commands	User Code + # + 80 + Time Window, Open/Close Schedule, Holidays, Timed Event, or Access Schedule	Create or edit time windows, open/close schedules, holidays, timed events and/or access schedules

The following system user levels may enter the above commands:

Authorization Level	User Name	Commands						
		#73	#74	#75	#77	#78	#79	#80
	Installer	X	X	X	X	X	X	X
1	Master	X	X	X	X		X	X
2	Manager	X	X	X				
3	Operator A	X	X					
4	Operator B	X	X					
5	Operator C	X	X					
6	Duress	X	X					

A complete description of the user commands is provided in the following paragraphs.

Access Control

The access control commands may be used to directly control access points or to add, remove, or edit cards in the system's cardholder database. The access control commands may be used as follows:

#73

The #73 command (if enabled for a keypad) may be used to grant entry or exit through an access point in the partition that the keypad is connected to. The access point will automatically relatch after the time interval set during system programming. For the #73 command to be accepted, the following conditions must exist.

- The keypad must be attached to the partition where the access point is located.
- If the partition is armed and Armed Restriction is in effect, the user must be authorized to disarm the partition.
- The user must have access to the partition at the time the command is entered.
- The VISTA user number must be assigned to a card with an access group assignment which includes the point and partition in which the keypad being used.
- The request will be denied if the access group, that allows the user access to a point, is disabled.
- The command must have been enabled using the procedures in *Section 5: Programming*.

Enter the #73 command as follows:

User Code + # + 73

The access point is unlatched for the time period that was defined during system programming.

#74

The #74 command may be used to grant entry or exit through any access point. The access point will automatically relatch after the time interval that was set during system programming. For the #74 command to be accepted, the following conditions must exist.

- If the partition is armed and Armed Restriction is in effect, the user must be authorized to disarm the partition.
- The VISTA user number must be assigned to the partition to which the keypad belongs.
- The VISTA user number must be assigned to a card with an access group assignment which includes the point to which access is being requested.
- The VISTA user number does not have to be assigned to the partition to which the access point belongs to be granted access, but if not, he/she will be denied access while the partition is armed and an armed restriction has been programmed.

Enter the #74 command as follows:

User Code + # + 74

The following message is displayed on the keypad:

Access Point	
00-31	01

Enter two digits (from 01 through 15) that corresponding to the access point number where entry or exit is to be allowed.

NOTE: When using the VistaKey, entries between 16 and 31 are invalid and will not cause any action.

Press the [✲] key to accept the entry. The following message is displayed on the keypad:

```
Entry or Exit
Entry                0
```

Enter **0** for entry or **1** for exit. The access point is unlatched for the time period that was defined during system programming with the "Door Open Time" and the "Relatch" option settings.

#75

The #75 command may be used to change the state (grant, bypass, or protect) of any access point. For the #75 command to be accepted, the following conditions must exist.

- If the partition is armed, Armed Restriction is in effect, and the user issues an access command, the user must be authorized to disarm the partition for the command to be accepted.
- The user must have a level assignment of Installer, Master, or Manager.
- The user must be assigned to the access point's partition to protect or bypass the access point.
- The VISTA user number must be assigned to the partition to which the keypad belongs.
- The VISTA user number must be assigned to a card with an access group assignment that includes the point to which access is being requested.
- The VISTA user number does not have to be assigned to the partition to which the access point belongs to be granted access, but if not, he/she will be denied access while the partition is armed when an armed restriction has been programmed.

Enter the #75 command as follows:

User Code + # + 75

The following message is displayed on the keypad:

```
Access Point
00-31                01
```

Enter two digits (from 01 through 15) that corresponding to the access point number where a change of state is desired.

NOTE: When using the VistaKey, entries between 16 and 31 are invalid and will not cause any action.

Press the [✲] key to accept the entry. The following message is displayed on the keypad:

```
DOOR COMMAND
NONE                 0
```

Enter one digit corresponding to the state desired. Valid entries are as follows:

0 = NONE – Has no effect on the current access point status.

1 = GRANT – Grants access through the access point. The access point is unlatched for the time period that was defined during system programming with the "Door Open Time" and the "Relatch" option settings.

2 = PROTECT – Places the access point into its normal operating state. This entry is used when you want to place an access point that is in the bypass state into its normal operating state. When an access point is protected, only valid cardholders can access it.

3 = BYPASS – Places the access point into the bypass state. While the access point is in the bypass state, the locking mechanism is unlocked, no forced-door or door-open-too-long alerts are generated, and any requests to enter or exit are ignored (the

door is already unlocked). The bypass state remains in effect until ended by receipt of the protect entry (above) or until the bypass is ended by a time window, action command, or timed event.

Press [*] to accept the entry. The selected action takes effect.

#79

The #79 command is used to add, remove, or edit cards in the system's cardholder database. For instructions on using this command, refer to "Performing Access Control Card Functions" in this section.

#77 Output Device Control

The #77 Output Device Control is used to activate outputs, bypass zones, activate access control commands, etc. under operator control. The actions that may be activated by the operator are relay commands, arm/disarm commands, zone bypassing commands, open/close access conditions, and access control commands. For the #77 command to be accepted, the following conditions must exist.

- The user must have a level assignment of Installer or Master.
- If the partition is armed, Armed Restriction is in effect, and the user issues an access command, the user must be authorized to disarm the partition for the command to be accepted.
- The user must be assigned to the access point's partition to protect, bypass, or lock the access point or to set it to exit only.
- To arm or disarm a partition, the user must be assigned to that partition.
- The VISTA user number must be assigned to the partition to which the keypad belongs.
- The VISTA user number must be assigned to a card with an access group assignment that includes the point to which access is being requested.
- The VISTA user number does not have to be assigned to the partition to which the access point belongs to be granted access, but if not they will be denied access while the partition is armed when an armed restriction has been programmed.

Enter the #77 command as follows:

User Code + # + 77

The following message is displayed on the keypad:

```
      ACTION ?
RELAY ON          01
```

Enter the two-digit Action Number that corresponds to the action desired.

The action codes are the events that are to take place immediately. 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.

Table 5-1: Action Codes provides a listing of the "Action Codes" (desired actions) used when programming keypad-driven events.

NOTE: Action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only) disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.

Press the [*] key to accept the entry.

An additional keypad display prompts you to enter the specifier (i.e., relay number, partition number, etc.) for the action selected. Enter the specifier.

Press the [*] key to accept the entry. The following display apprears:

↓ Action Number

```
01   Are You Sure?
 1=YES   0=NO          0
```

Press **1** to accept your entries for action and action specifier, or enter **0** to cancel your entries.

Press the [*] key to continue. The action specified (or cancellation) takes effect and the following display appears:

```
Quit?
 1=YES   0=NO          0
```

Press **1** if you are finished entering actions, or press **0** if you want to enter additional actions.

Press the [*] key to accept your entry. If you entered 1, the program exits. If you entered 0, the system returns to the "Action ?" prompt.

#78 Access Control Test

The #78 command is used to perform testing on access points as previously described in the *Quick Installation* and *Detailed Installation* sections.

#80 Schedule Control

The #80 command is used to define or change system time windows and/or time-driven events. For instructions on using this command, refer to the procedures under *Scheduling Options* descriptions in your alarm system manual.

Performing Access Control Card Functions

Access control card functions are performed using the #79 Card Function Programming. #79 Card Function Programming provides capabilities for modifying the card database contained in the alarm system panel by adding cards, editing cards, and/or deleting cards. Cards can be added or deleted individually or by groups. To aid in keeping track of cardholders assigned to the system, we recommend that you copy the Cardholders Worksheet, at the end of this section, and fill it in when cards are assigned or re-assigned.

Keep the following items in mind while enrolling cards into the system:

- Any cards enabled for executive privileges have complete access to every access point, are permitted to disarm any partition in the system, and are always active regardless of timed event schedules for their access group. Only Expire Use and Expire Month affect the life of a card given executive privileges. Also, cards programmed with executive privilege need not be mapped to an access group unless an access group has specific events associated with it that you want to apply to the cards.
- VISTA User Number: Any VISTA user numbers that will be used for assignment to a card or cards, must be defined before performing #79 Card Function Programming. While performing access control card functions, only VISTA user numbers that have been priviously defined will be accepted. To assign VISTA user numbers, refer to the procedures in your alarm system manual.
- VISTA User Number field: Cards not mapped to valid VISTA user numbers or left at the default value 000 are permitted access to and able to disarm partitions that the card's access group is given access to in Access Group Programming. To prevent a card from accessing a door when the system is armed, you must enable the Armed Restriction (see the *Programming* section).

  Cards mapped to valid VISTA users in the system always have access to an access point and always are able to disarm a partition that the card's access group is given access to in Access Group Programming. See the two examples below.

1. A card's access group is given access to a point in Access Group Programming. Partition Armed Restriction is not programmed. The following is true:

Card	Executive Privilege	VISTA User Number	Access Through Access Point if System Armed	Disarm System
001	Yes	000	Yes	Yes
002	Yes	*Any Valid	Yes	Yes
003	No	000	Yes	Yes
004	No	*Any Valid	Yes	Yes

* "Any valid" means that the card is tied to a VISTA user who also has access to the partition to which the access point is assigned.

2. A card is given access to a point in Access Group Programming. Partition Armed Restriction **is** programmed. The following is true:

Card	Executive Privilege	VISTA User Number	Access Through Access Point if System Armed	Disarm System
001	Yes	000	Yes	Yes
002	Yes	*Any Valid	Yes	Yes
003	No	000	No	No
004	No	*Any Valid	Yes	Yes

* "Any valid" means that the card is tied to a VISTA user who also has access to the partition.

To begin #79 Card Function Programming, enter **User Code** + **#79**. The following prompt appears:

Access Point 00

Enter the number (01-15) of the access point (door) for which you want to change card data.

Press **[*]** to accept the entry.

The "Add Card?" Prompt appears. To add a card or edit a card by using a card swipe, go to the "Adding Cards" paragraph below. If you do not want to Add a card or edit a card by using a card swipe, press [0] on the keypad to advance the display to another choice. When the choice desired is displayed, stop pressing [0] and refer to the corresponding paragraph in this section for procedural instruction. The order in which the choices are displayed is:

Add Card?
Edit Card?
AUTO Delete?
BLOCK Delete?
MANUAL Delete?
Quit Card Mode?

Adding Cards

```
Add Card?
1=Yes  0=No        0
```

Press **1** to enroll a new card or edit a card by using a card swipe. Press **0** advance to the Edit Card function. When 1 is entered, the following prompt is displayed.

NOTE: When you use this procedure to edit a card, the display content is based on the definitions previously made for the card being edited, and does not necessarily match the examples provided here.

```
SWIPE CARD
xxx-xx-xxxxxxx
```

Swipe card or manually enter the (12-digit) card code to be enrolled or edited. If you swipe a card, the keypad displays a 3-digit VISTA card ID number preceding "SWIPE CARD" on the top line of the display and the 12 digits of information contained on the card in the second line of the display. Note that if the card you swiped has already been enrolled, the keypad sounds a double beep notifying you that the card has already been enrolled and your entries will be for editing the existing card data. The characters in the second line of the display have the following meaning.

Digits 1 through 3 = 3-digit facility code
Digits 4 and 5 = 2-digit RCM code
Digits 6 through 12 = 7-digit card ID code

Press **[*]** to accept the entry.

NOTE: If this is the first card in this programming session, the alarm system advances to the next prompt. If this is not the first card in this session, the system performs one of the following steps:

a. If block entry **was not selected** on the first card, the system advances to the next prompt.
b. If block entry **was selected** on the first card, the system stores the card number and all other data defined for the first card, and then advances to the "Quit?" prompt.

↓ VISTA Card ID Number

```
001 Exec Priv?
NOT ENABLED        0
```

Enabling Executive Privilege for this cardholder enables the cardholder to access any access point and disarm the access point's partition (if armed) at any time regardless of whether the cardholder's access group is enabled via scheduling or whether his access group is enabled to enter or exit through any of the access points. The only reason that a cardholder with executive privilege is prevented from gaining access through an access point would be if his card has expired via usage or date. Disabling Executive Privilege allows cardholders entry through access points only if the following conditions exist:

- The access point has been programmed to accept the cardholder's access group.
- The cardholder's access group is enabled at the time of the card swipe (via scheduling, event/action or action selector), PIN entry (code + # + 73), or RF button remote depression.
- The cardholder's card has not expired.

Enter **1** to provide the cardholder with executive privileges, or **0** for no executive privileges.

NOTE: It the card belongs to an access group that has executive privilege enabled, this feature can be inherited from the access group; however, only executive privilege assigned to a card will be accepted when the VistaKey is operating in RCM.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Trace?
NOT ENABLED      0
```

The Trace feature allows the cardholder to be monitored by logging his entry/exit grants and denials in the log and (if programmed) dialing out and sending a report to central station. Note that a card may also inherit a trace enable from its access group assignment. A card is traced if any access group that it is assigned to has trace enabled.

NOTE: If a card has expired (from number of uses or date) and trace is enabled, any attempt to use the card will be logged and dial out (if enabled) as user U999. When a card expires, it remains in the database so that it may be reinstated if desired.

Enter **1** to trace the cardholder, or **0** for no trace.

Press **[*]** to accept the entry.

```
ACS GRP?1 2 3 4 5 6 7 8
HIT 0-8
```

Each cardholder must belong to at least one access group. The access group provides the cardholder with certain privileges afforded to all cardholders that belong to that access group. If a cardholder belongs to more than one access group, he is afforded all the privileges of all the access groups he belongs to. The access groups also determine which access point(s) the cardholder has access to and at what times according to the schedule his access group is enabled.

Press **0** to toggle all access groups on or off; or press keys **1**-**8** to toggle the letter "x" under the access group numbers on or off.

Press **[*]** to accept the entry.

NOTE: Numbers toggle. For example, pressing 1 turns group 1 on and pressing 1 again turns group 1 off.

↓ VISTA Card ID Number

```
001 Expire use?
UNLIMITED USE    00
```

"Expire use" defines whether the cardholder access privileges are to expire with usage. Enter 00 for unlimited use. Otherwise, enter a number between 01 and 14. Entering a number between 01 and 14 allows that many entry access grants for this cardholder. Egress grants have no effect on the usage count. Entering 15 automatically expires the card and no entry grants are permitted even if the cardholder has executive privilege. Expiring a card will NOT delete it from the card database; the card retains its card ID#.

NOTE: If you set a card to expire with use and also set the same card to expire by time ("Expire Month" below), then the card will expire on the first event to occur.

Enter a number from **00** to **15**.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Expire Month
NO EXPIRATION    00
```

Enter two digits from **00** to **15**. The digits entered provide the following expiration functions:

00 = Normal (no expiration)	08 = August
01 = January	09 = September
02 = February	10 = October
03 = March	11 = November
04 = April	12 = December
05 = May	13 = End of Day
06 = June	14 = End of Week (Sunday)
07 = July	15 = End of Month

NOTES:

- Cards expire at midnight for month, end of day, end of week, and end of month selections.
- If you set a card to expire by time and also set the same card to expire with use ("Expire Use?" above), then the card will expire on the first event to occur.

Press **[*]** to accept the entry.

If you entered 01-12, the system displays the "Day of Month" prompt.

If you entered 00, or 13-15 the system advances to the "Vista User #" prompt.

↓ VISTA Card ID Number

```
001 Day of Month
                 00
```

Enter day of the month. Note that the card expires at midnight of the day that is entered.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Vista User#
                000
```

Enter a three-digit VISTA User #.

The VISTA user number may be used to allow a cardholder access to an armed partition even if the cardholders access group is restricted for that partition. Additionally, the VISTA User # can be used to allow this cardholder to use wireless keyfobs to grant access and egress through his allotted access points.

NOTES:

- Cardholders with VISTA user number of 000 can disarm partitions to gain entry if they belong to an access group that doesn't have an Armed Restriction for that partition. See "Setting Up Access Groups" in the *Programming* section of this manual for more information.
- The system only accepts VISTA user numbers that have been defined prior to entering #79 Card Function Programming.
- Cardholders with VISTA user number of 000 will be identified as U999 if the trace option is selected.
- The partition rights and privileges of the VISTA user assigned should be consistent with the partition rights and privileges assigned to the card and to the access group to which the card belongs.
- If you assign a VISTA user number to a cardholder and subsequently delete that VISTA user number from the panel, the

cardholder retains all rights and privileges that the VISTA user number provided. These rights and privileges remain in effect until such time as the cardholder is deleted from the system or the card expires.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 ACS Event?
Never Invoke        00
```

Enter two digits from the list below for the access point-related event desired. Acceptable entries have the following meaning:

00 = never invoke	06 = egress grant
02= access request	07 = any grant
03 = egress request	08 = access denied
04 = any request	09 = egress denied
05 = access grant	10 = any denial

Press **[*]** to accept the entry.

NOTES:

- If you selected 00 "never invoke," the system advances to the "Block Entry" prompt.
- For the ACS Event to occur, the card must be swiped at the access point defined in the following prompt.

↓ VISTA Card ID Number

```
001 Access Point?
(01-15)             00
```

Enter 1 through 15 for the access point number corresponding to the event defined above.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 ACTION?
None                00
```

Enter two digits defining the action desired. For acceptable entries and their meanings, see *Table 5-1: Action Codes* in the *Programming* section of this manual.

NOTES:

- For the Action to occur, the ACS Event (defined above) must have been invoked by a card swipe at the access point defined in the above prompt.
- Actions that arm or disarm a partition will only be performed if the VISTA user number (for the card) is assigned to the partition to be armed or disarmed.
- Action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only) disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.

Press **[*]** to accept the entry.

In response to the action entered, the system displays a message asking for additional information based on the action you selected. For example, if the action you selected was **01** (relay on), the system presents a message asking for a relay number. Respond to the message and then press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Block Entry?
1=YES   0=NO        0
```

Block enrollment (entry) allows you to enroll numerous cards with the same previously entered data. If the card data to be entered are significantly different from one another, then answer "NO" and enter each card's data individually by swiping the card and entering data alternately. Otherwise, enter "yes" to duplicate card data for every card swiped. The sequence for block enrollment is: swipe card, press [✲], enter data, swipe card, press [✲], swipe card, press [✲],... swipe card, press [✲], quit. The sequence for individual data entry is: swipe card, press [✲], enter data, swipe card, press [✲], enter data ... swipe card, press [✲], enter data, quit.

Enter **1** to swipe additional cards with identical data definitions, or **0** if you will not be entering additional cards with identical data definitions.

```
Quit?
1=YES   0=NO        0
```

Enter **1** or **0**.

If you enter 1, the system advances to the "Quit Card Mode?" prompt.

If you enter 0, the system returns to the "SWIPE CARD" prompt.

Editing Cards

This mode allows you to edit cards by entering the card number. To edit cards based on a card swipe or the 12-digit card code, refer to the "*Adding Cards*" procedure.

```
Edit Card
1=Yes   0=No
```

Enter **1** or **0**.

If you enter 1, the system advances to the next prompt.

If you enter 0, the system advances to the "Auto Delete" prompt.

NOTE: Cards may also be edited by swiping them past the card reader or entering the 12-digit card code. To edit cards based on a card swipe or the 12-digit card code, refer to the "*Adding Cards*" procedure in this section.

```
Card #
1-250  0=Quit      001
```

Enter a valid card number from **001** to **250** or **000** to quit.

If you entered a number from 001 to 250, the system advances to the next prompt.

If you entered 000, the system advances to the "Quit Card Mode?" prompt.

NOTE: If you enter an invalid card number, "ERROR" is displayed. An invalid card number is any number that has not already been added into the system.

Press **[✲]** to accept the entry.

NOTE: NOTE: The display content while editing cards is based on the definitions previously made for the card being edited, and will not necessarily match the examples provided in this procedure. If the card has not been previously defined, an error message is displayed notifying you to enter a different number.

↓ VISTA Card ID Number

```
001 Exec Priv?
NOT ENABLED         0
```

Enabling Executive Privilege for this cardholder enables the cardholder to access any access point and disarm the access point's partition (if armed) at any time regardless of whether the

cardholder's access group is enabled via scheduling or whether his access group is enabled to enter or exit through any of the access points. The only reason that a cardholder with executive privilege is prevented from gaining access through an access point would be if his card has expired via usage or date. Disabling Executive Privilege allows cardholders entry through access points only if the following conditions exist:

- The access point has been programmed to accept the cardholder's access group.
- The cardholder's access group is enabled at the time of the card swipe (via scheduling, event/action or action selector), PIN entry (code + # + 73), or RF button remote depression.
- The cardholder's card has not expired.

Press **1** to provide the cardholder with executive privileges, or **0** for no executive privileges.

NOTE: It the card belongs to an access group that has executive privilege enabled, this feature can be inherited from the access group; however, only executive privilege assigned to a card will be accepted when the VistaKey is operating in RCM.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Trace?
NOT ENABLED        0
```

The Trace feature allows the cardholder to be monitored by logging his entry/exit grants and denials in the log and (if programmed) dialing out and sending a report to central station. Note that a card may also inherit a trace enable from its access group assignment. A card is traced if any access group that it is assigned to has trace enabled.

NOTE: If a card has expired (from number of uses or date) and trace is enabled, any attempt to use the card will be logged and dial out (if enabled) as user U999. When a card expires, it remains in the database so that it may be reinstated if desired.

Press **1** to trace the cardholder, or **0** for no trace.

Press **[*]** to accept the entry.

```
ACS GRP?1 2 3 4 5 6 7 8
HIT 0-8   x x x x x x x x
```

Each cardholder must belong to at least one access group. The access group provides the cardholder with certain privileges afforded to all cardholders that belong to that access group. If a cardholder belongs to more than one access group, he is afforded all the privileges of all the access groups he belongs to. The access groups also determine which access point(s) the cardholder has access to and at what times according to the schedule his access group is enabled.

Press **0** to toggle all access groups on or off; or press keys **1**-**8** to toggle the letter "x" under the access group numbers on or off.

Press **[*]** to accept the entry.

NOTE: Numbers toggle. For example, pressing 1 turns group 1 on, and pressing 1 again turns group 1 off.

↓ VISTA Card ID Number

```
001 Expire use?
UNLIMITED USE     00
```

"Expire use" defines whether the cardholder access privileges are to expire with usage. Enter 00 for unlimited use. Otherwise, enter a number between 01 and 14. Entering a number between 01 and 14 allows that many entry access grants for this cardholder. Egress grants have no effect on the usage count. Entering 15 automatically expires the card and no entry grants are permitted even if the cardholder has executive privilege. Expiring a card will NOT delete it from the card database; the card retains its card ID#.

NOTE: If you set a card to expire with use and also set the same card to expire by time ("Expire Month" below), then the card will expire on the first event to occur.

Enter a number from **00** to **15**.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Expire Month
NO EXPIRATION     00
```

Enter two digits from **00** to **15**. The digits entered provide the following expiration functions:

00 = Normal (no expiration)	08 = August
01 = January	09 = September
02 = February	10 = October
03 = March	11 = November
04 = April	12 = December
05 = May	13 = End of Day
06 = June	14 = End of Week (Sunday)
07 = July	15 = End of Month

NOTES:

- Cards expire at midnight for month, end of day, end of week, and end of month selections.
- If you set a card to expire by time and also set the same card to expire with use ("Expire Use?" above), then the card will expire on the first event to occur.

Press **[*]** to accept the entry.

If you entered 01-12, the system displays the "Day of Month" prompt.

If you entered 00 or 13-15 the system advances to the "Vista User #" prompt.

↓ VISTA Card ID Number

```
001 Day of Month
                  00
```

Enter day of the month. Note that the card expires at midnight of the day that is entered.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

```
001 Vista User#
                 000
```

Enter a three-digit VISTA User #.

The VISTA user number may be used to allow a cardholder access to an armed partition even if the cardholders access group is restricted for that partition. Additionally, the VISTA User # can be used to allow this cardholder to use wireless keyfobs to grant access and egress through his allotted access points.

NOTES:

- Cardholders with VISTA user number of 000 can disarm partitions to gain entry if they belong to an access group that doesn't have an Armed Restriction for that partition. See "Setting Up Access Groups" in the *Programming* section of this manual for more information.
- The system only accepts VISTA user numbers that have been defined prior to entering #79 Card Function Programming.
- Cardholders with VISTA user number of 000 will be identified as U999 if the trace option is selected.
- The partition rights and privileges of the VISTA user assigned should be consistent with the partition rights and privileges assigned to the card and to the access group to which the card belongs.
- If you assign a VISTA user number to a cardholder and subsequently delete that VISTA user number from the panel, the cardholder retains all rights and privileges that the VISTA user number provided. These rights and privileges remain in effect until such time as the cardholder is deleted from the system or the card expires.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

001 ACS Event?	
Never Invoke	00

Enter two digits from the list below for the access point-related event desired. Acceptable entries have the following meaning:

00 = never invoke	06 = egress grant
02= access request	07 = any grant
03 = egress request	08 = access denied
04 = any request	09 = egress denied
05 = access grant	10 = any denial

Press **[*]** to accept the entry.

NOTES:

- If you selected 00 "never invoke," the system advances to the "Block Entry" prompt.
- For the ACS Event to occur, the card must be swiped at the access point defined in the following prompt.

↓ VISTA Card ID Number

001 Access Point?	
(01-15)	00

Enter 1 through 15 for the access point number corresponding to the event defined above.

Press **[*]** to accept the entry.

↓ VISTA Card ID Number

001 ACTION?	
None	00

Enter the two-digit Action Number defining the action desired. For acceptable entries and their meanings, see *Table 5-1: Action Codes* in the *Programming* section of this manual.

NOTES:

- For the Action to occur, the ACS Event (defined above) must have been invoked by a card swipe at the access point defined in the above prompt.
- Actions that arm or disarm a partition will only be performed if the VISTA user number (for the card) is assigned to the partition to be armed or disarmed.

- Action codes 60 (AP Exit Only), 66 (AP Group Exit Only), or 72 (AP Partition Exit Only) disable the entry reader at the access point. The reader will remain disabled until a command is received (via a keypad command or event) to protect the access point.

Press **[*]** to accept the entry.

In response to the action entered, the system displays a message asking for additional information based on the action you selected. For example, if the action you selected was **01** (relay on), the system presents a message asking for a relay number. Respond to the message displayed, and then press **[*]** to accept the entry.

```
Quit?
1=YES   0=NO          0
```

Press **1** or **0**.

If you press 1, the system advances to the "Quit Card Mode?" prompt.

If you press 0, the system returns to the "Exec Priv?" prompt.

Auto Delete

```
Auto Delete?
1=Yes   0=No          0
```

Press **1** or **0**.

If you press 1, the system advances to the next prompt.

If you press 0, the system advances to "Block Delete?" prompt.

```
SWIPE CARD
xxx-xx-xxxxxxx
```

Swipe card or enter card number to be deleted. The card number and VISTA card ID number to be deleted aredisplayed on the keypad. Note that if the card swiped is not found in the system database, the card number displayed and VISTA card ID number are shown as zeros.

Press **[*]** to accept the entry.

If the card is found in the system database, the system advances to the "Are You Sure?" prompt.

If the card is not found in the system, the following "Card not Found" prompt is displayed.

```
Card not Found
* to continue
```

Press **[*]** to continue. The system advances to the "Quit?" prompt.

```
Are You Sure?
1=YES   0=NO          0
```

Press **1** or **0**.

If you press 1, the system marks the card database that the card is deleted.

If you press 0, the system advances to the "Quit?" prompt.

Press **[*]** to accept the entry.

Quit? 1=YES 0=NO 0

Press **1** or **0**.

If you press 1, the system advances to the "Quit Card Mode?" prompt.

If you press 0, the system returns to the "Swipe Card" prompt.

Press **[*]** to accept the entry.

Block Delete

Block Delete? 1=Yes 0=No 0

Press **1** or **0**.

If you press 1, the system advances to the next prompt.

If you press 0, the system advances to the "Manual Delete?" prompt.

Delete from Card 1-250 0=Quit 001

Enter the 3-digit number corresponding to the beginning (lowest) card number for the deletion. If you enter 000, the system advances to the "Quit Card Mode?" prompt.

Press **[*]** to accept the entry.

To Card 1-250 0=Quit 000

Enter the 3-digit number corresponding to the ending (highest) card number for the deletion.

NOTE: If this number is not greater than the number entered as the "Delete from Card" above, no cards will be deleted.

Press **[*]** to accept the entry.

Are you sure? 1=Yes 0=No 0

Press **1** or **0**.

If you press 1, the system marks the card database that these card numbers are deleted from the card database and returns to the "Delete from Card" prompt.

If you press 0, the system returns to the "Delete from Card" prompt without marking any cards in the database for deletion.

Press **[*]** to accept the entry.

Manual Delete

MANUAL Delete? 1=YES 0=NO 0

Press **1** or **0**.

If you press 1, the system advances to the next prompt.

If you press 0, the system advances to "Quit Card Mode?" prompt.

Delete Card ID# (001-250) 0=Quit 0

Enter a number from **001** to **250** or **000** to quit.

If you entered a number from 001 to 250, the system advances to the next prompt.

If you entered 000, the system advances to the "Quit Card Mode?" prompt.

Press **[*]** to accept the entry.

Are you sure? 1=Yes 0=No

Press **1** or **0**.

If you press 1, the system marks the card database that the card is deleted and the system returns to the "Delete Card ID#" prompt.

If you press 0, the system returns to the "Delete Card ID#" prompt without deleting the card from the database.

Press **[*]** to accept the entry.

Quit Card Function Programming

Quit Card Mode 1=Yes 0=No

Press **1** or **0**.

If you press 1, the system exits card function programming.

If you press 0, the system returns to the "Add Card?" prompt.

CARDHOLDERS WORKSHEET

NAME	CARD NUMBER	EXEC PRIV	TRACE	ACCESS GROUP	EXPIRE USE	EXPIRE MONTH/ DAY	VISTA USER NO.	ACS EVENT	ACCESS POINT	ACTION
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						
		Y N	Y N	1 2 3 4 5 6 7 8						

SECTION 7

System Testing

In This Section

General Information

This section provides information about system testing, the LED indicators and jumper in the VistaKey module, improper switch setting indications, and the DSM supervision fault.

System Testing

This paragraph provides information that allows you to make certain that the access groups that you have defined are granted access during the time periods that you have defined without triggering system alarms. By successfully completing the below procedures you will have verified that the access control portion of your system is operational.

1. To test access groups that are enabled and disabled by timed events, you must adjust the control panel's real-time clock accordingly. For example: If you have an access group enabled between the hours of 8:00 AM and 5:00PM, you must set the clock to 7:59 AM and then wait 1 minute.
2. Check to make sure the access group is granted access by swiping a card in that group.
3. Change the real-time clock to 4:59 PM and wait 1 minute.
4. Check to make sure the access group is not granted access (disabled) by swiping a card in that group.
5. Repeat steps 1 through 4 for each access group.
6. Once all access groups are tested, reset the real-time clock to the current time. Any access groups controlled by timed events that you want to turn on for immediate use can be enabled via the #77 mode. All access groups controlled by timed events will later be disabled when scheduled.

Refreshing Time Initated Actions

During system installation and testing, you may desire to refresh the actions that are based on time windows and/or schedules. When a refresh occurs, actions driven by windows defined for the current day and spanning the current time are activated in the same manner as if the window became active by a normal occurrence. The status of time initiated actions are refreshed in response to each of the following events:

NOTE: The refresh does not take an entire weekly schedule into account when determining the status of action objects. It refreshes windows defined for the current day only.

- Changing any component of the Time/Date via #63 user function. To have the refresh occur, you must actually change the time and/or date.
- Leaving #80 Schedule Mode. The refresh occurs even if you have not made any changes in the #80 Schedule Mode.

- Leaving Keypad Programming Mode. The refresh will occur even if you have not made any changes in the Keypad Programming Mode.
- Any time the panel hangs up after reaching ring count while trying to establish a connection with the downloader. This refresh will occur whether or not the panel established a connection with the downloader.
- On powerup.
- When daylight savings adjustment occurs.

VistaKey Module LEDs and Jumper

The VistaKey contains a green LED, red LED, and a jumper. The green LED indicates the VistaKey state, the red LED indicates theVistaKey door control relay state, and the jumper is for future use. For detailed explanation, refer to the following paragraphs.

Green LED

The green LED provides a repeating series of blinks that indicate the current state of the VistaKey. Each series of blinks have the following meanings:

# of Blinks in Series	Module State	# of Blinks in Series	Module State
1	Reset (Future Use)	8	RTE
2	RCM Mode (Future Use)	9	RTE Grant In Process
3	Protected	10	Open Alarm
4	Bypassed	11	Timeout Alarm
5	Locked	12	Exit Only
6	Grant In Process	13	Pre-Alarm
7	Denied In Process		

Red LED

The red LED indicates the current state of the VistaKey dorr control relay. When the red LED is on, it indicates the VistaKey dor control relay is active (energized).

Jumper

The jumper is located in the VistaKey module between TB 3 and the K 1 door control relay. This jumper is for future use and should be shorting the two pins closest to the door control relay. Proper module operation cannot be assured, in all operating conditions, if this jumper is moved or removed from the VistaKey module.

Improper Address Switch Position

During system usage, if the module experiences a loss of power or if the address switch on a VistaKey module is changed to an improper address, the panel logs an ACLO MOD (AC Loss Module) event. If this event is logged and power is applied to the module, check that the module's address switch is set to the proper address.

DSM Supervision Fault Clearing

A DSM check message is displayed on the keypad and is logged during system usage if a fault develops on the polling loop connection. Note that the DSM check message can take up to one minute to clear from the keypad display after the fault has been corrected.

SECTION 8

Event Log

In This Section

General Information

This section provides the additional event log entries that are added to the alarm panel when a VistaKey is connected. Below is a list of the events sent to the central station (CS) and the events logged into the alarm panel.

Central Station Reporting

The following list contains all additional events that may be reported to the CS. The entires are grouped by event type. Note that event reporting can be enabled via the Access Dialer Enables (described in the *Programming* section of this manual).

ACS Alarms

Event	Code	Specifier
Duress Access Grant	124	User #
Duress Egress Grant	125	User #
Door Forced Open/Restore	423	DSM Zone #

ACS Troubles

Event	Code	Specifier
AC Loss at Module/Restore*	342	DSM Zone #
Door Propped/Restore	426	DSM Zone #
DSM Trouble/Restore	427	DSM Zone #
RTE Trouble/Restore	428	DSM Zone #

* If a module experiences a loss of power or if the address switch on a VistaKey module is changed to an improper address, the panel logs an ACLO MOD (AC Loss Module) event and the AC Loss will be reported. If this event is logged and power is applied to the module, check that the module's address switch is set to the proper address.

ACS Bypasses

Event	Code	Specifier
Access Point Bypass/Restore	577	DSM Zone # (Door Lock Is Open)

ACS System

Event	Code	Specifier
Module Reset	339	DSM Zone # (On Power-up)
Test Entry/Exit	607	DSM Zone #

ACS Trace

NOTE: For the events below, the ASC Group and/or Cardholder Trace must be on.

Event	Code	Specifier
Access Grant	422	User #
Access Denied	421	User #
Egress Grant	425	User #
Egress Denied	424	User #

NOTE: An Access Point Lock event is not logged or reported

Alarm Panel Logging

The following list contains all additional events that may be entered into the event log in the alarm panel. The entries are grouped by log category.

NOTE: The below events will only be logged if their types are enabled in alarm panel field 1*70. Refer to your alarm system installation and setup guide for additional information.

Alarm

Event	Log Entry	Specifier
Door Forced	DR FORCE	DSM Zone #
Door Forced Restore	DRFO RST	DSM Zone #

NOTE: The events below are only logged when the Access Group Trace or Card Trace options are enabled.

Access Grant	ACS GRT	[DSM Zone #] U [User #]
Access Denied	ACS DENY	[DSM Zone #] U [User #]
Egress Grant	EGR GRT	[DSM Zone #] U [User #]
Egress Denied	EGR DENY	[DSM Zone #] U [User #]

Check

Event	Log Entry	Specifier
Door Propped	DR DROP	DSM Zone #
Door Propped Restore	DRPO RST	DSM Zone #
DSM Trouble	DSM TRBL	DSM Zone #
DSM Trouble Restore	DSM RST	DSM Zone #
RTE Trouble	RTE TRBL	DSM Zone #
RTE Trouble Restore	RTE RST	DSM Zone #
AC Loss at Module*	ACLO MOD	DSM Zone #
AC Loss at Module Restore	ACRST MOD	DSM Zone #

* If a module experiences a loss of power or if the address switch on a VistaKey module is changed to an improper address, the panel logs an ACLO MOD event and the AC Loss will be reported. If this event is logged and power is applied to the module, check that the module's address switch is set to the proper address.

Bypass

Event	Log Entry	Specifier
Access Point Bypass	ACPT BYP	[DSM Zone #] U [User #]
Access Point Unbypass	ACPT UNB	[DSM Zone #] U [User #]

System

Event	Log Entry	Specifier
Module Reset	RES MOD	DSM Zone #

NOTE: An Access Point Lock event is not logged or reported

SECTION 9

Reduced Capability Mode

In This Section

General Information

To help ensure that a user has access in the rare event of a problem, the VistaKey contains a Reduced Capability Mode (RCM), which allows the system to operate on the card database stored in the VistaKey. The VistaKey automatically enters RCM in the event communication between the VistaKey and the alarm panel is lost for a period of two or more minutes (providing that the VistaKey has power applied). The RCM mode automatically ends within one minute after communications are restored.

Additionally, when you have a direct-wire computer connection and you request a download to the alarm panel using the downloader, system-wide RCM will occur 2 minutes after the direct-wire computer connection is established, and remains until 1 minute after the connection is terminated. While in the Reduced Capability Mode, the VistaKey recognizes and grants access for all cards authorized to enter through an access point (without regard to time schedules).

The card database is downloaded from the alarm panel to the VistaKey within ten minutes of leaving #79 mode, an alarm panel download, VistaKey module powerup, or reaching 12 midnight. Therefore, if the system should enter RCM while you are working on the card database, it is possible that your recent changes may not have been downloaded and the VistaKey is operating on the card database as it existed before you started working on it.

RCM Description

When the VistaKey has entered RCM, the alarm panel keypad displays the zones controlled by the VistaKey as being in “Check,” and the system grants access at the access point being controlled by the VistaKey. While operating in RCM, the VistaKey has the following capabilities and limitations:

- On entering RCM, the door/access point is put into the protect/normal mode regardless of the state it was in previously (e.g., locked, bypassed, or exit only).
- While in RCM, the VistaKey cannot grant a card access based on executive privilege that it would normally inherit from its access group assignment; however, it will do this based on executive privilege assigned to the card itself.
- While in RCM, access restrictions based on time schedules, access group armed partition restriction, and access group disables are waived.
- While in RCM, the VistaKey can perform an access point grant, protect, or bypass card action based on the information in the card database. Hence, you can create cards that will provide an access point grant, protect, or bypass while the VistaKey is in RCM.
- If a card disarms an alarm panel partition during normal operation, it will not disarm the partition while operating in RCM.

- The VistaKey recovers from RCM within 1 minute of having its mux loop communication restored.
- The door/access point is restored to its previous state (e.g., locked, bypassed, or exit only) when RCM ends.

APPENDIX A

Glossary

A

Access Card - A card, generally the size and shape of a credit card, containing encoded data and used for controlling access. This system uses proximity-encoded cards.

Access Control - Allowing the right person through the right doors at the right time based on: 1) What they have, 2) What they are, and/or 3) What they know.

Access Group - A group of individuals who share common access privileges regarding associated access points (doors) and times. The access group defines the access privileges of the individuals. All members of an access group have identical access privileges.

Access Level - The type of access permissions assigned to a cardholder.

Access Point - A collection of card readers, zones, triggers, and door control relays committed to the control and monitoring of the door control hardware at a single point of passage.

Access Privileges - The rights allocated to an individual that define his/her access capabilities. Access privileges consist of the specifications of when and where a person may gain access or be allowed egress from a controlled area.

B

Bypass (Access Point) - When an access point is placed in Bypass mode, the locking mechanism is unlocked, no forced-door or door-open-too-long alerts are generated, and any requests to exit are ignored (the door is already unlocked). The access control industry also refers to this condition as “free access”.

C

Card Reader - A device used by cardholders to identify themselves to the system. The card reader reads the cardholder’s access card so that the access privileges of the cardholder may be examined in order to determine if the cardholder should be allowed to pass into the protected area.

Cardholder - An occupant of a premises who has been issued an access card or access code thst is used to request passage through protected access points within the premises.

Committed Resource - A resource, such as a reader or relay, that is directly assigned to an access point. The committed resource can no longer be controlled or monitored as an individual item. A committed relay, for example, is used to control the door to which it is assigned.

D

Door Control Hardware - The equipment installed at an access point to control the entry and exit of cardholders. The type of door control hardware you should choose depends in part on the level of security you want for each access point. There are many types of door control hardware available, as well as different ways to configure them.

Door Control Relay - The door control relay is an electromechanical switch that is used to control the flow of electricity to the door locking mechanism. The door control relay provides a Form C dry contact set for an output. In this way, it can be used to introduce or eliminate current flow to an external device.

Door Open Time - The amount of time that the door-locking device will be kept in the unlocked (open) status following a valid card swipe at the card reader or RTE, unless a relatch condition occurs.

Door Propped – The zone fault condition that is generated when a door is still open after the sum of the door open time and the alarm timeout has been reached. This condition can only occur when a DSM monitors the door.

Door Strike - An electromechanical locking device typically installed in a doorframe to enable locking and unlocking of the door by electrical or electronic means. Internally, the device consists of a solenoid to which power is applied, causing a plunger to move linkage, which releases a locking mechanism.

DSM (Door Status Monitor) - A zone in an access control system committed to the monitoring of a door sense switch. The door sense switch reflects the state of the door (open or closed) and also allows the system to determine if the door has been forced open or held open too long.

E

Entry Reader - An input device installed on the entry side of an access point door. At this device, individuals are required to identify themselves to the system so that their access privileges may be examined in order to determine if they should be allowed to pass into the protected area. The term is "entry reader" because in most cases, the device is a card reader at which a cardholder must present his ID card.

EOLR Supervision (End-of-Line Resistor Supervision) - A mode that is used to detect when someone has cut or shorted a cable monitoring a zone, such as a door sense switch. A resistor can be placed in the zone's circuit at the protected point such that the controller can detect line trouble, in addition to fault and normal conditions.

Event/Action - An option programmed by the user that allows system functions to be linked to a system event. Upon the occurrence of the system event, the action is performed.

Executive Privileges - An option that can be granted to cardholders to allow them full access to all of the system access points.

Exit Only - One of the modes in which an access point may be configured to operate. In this mode, the access point only accepts exit requests. Any entry reader is ignored.

Exit Reader - An input device that is installed on the exit side of an access point door. At this device, an individual is required to identify him/herself to the system so that their access privileges may be examined in order to determine if they should be allowed to pass out of the protected area. (See also: Entry Reader)

F

Form C Relay Output - A Form C relay output is a configuration comprised of a Common terminal point, a Normally Open terminal point, and a Normally Closed terminal point. With the relay in a de-energized state, the Common and Normally Closed points are connected to each other, and the Common and Normally Open points are disconnected from each other. When the relay energizes, the Common and Normally Closed points disconnect from each other and the Common and Normally Open points connect to each other.

Free Access - See Bypass (Access Point)

H

Holiday - A component of time schedules that defines days of the work week when the "normal" work schedule does not apply to the premises. For example, Thanksgiving Day would be considered a holiday.

K

Keypad - Typically a 12-button arrangement of momentary push buttons used to transmit a code to the system based on a specific sequence of keystrokes. The keypad generally resembles a telephone keypad with respect to the relative positions and key name assignments.

L

Locked (Access Point) - A mode that latches the door of the access point. The access point's readers will be disabled for access control functions. The access point does not allow any accesses or egresses in the Locked mode.

M

Mag Lock (Magnetic Lock) - A large coil of wire mounted to a door frame, that when current is passed through the coil, creates a strong magnetic field. A large metal plate is also secured to the door, and is held tightly against the coil of wire by the strong magnetic field.

The door can be released (or "unlocked") by interrupting the flow of current through the coil, thereby removing the strong magnetic field.

O

Outputs - Auxiliary devices in an access control system that control external devices such as electronic locks, piezo sounders, or light indicators. These can consist of relay outputs (dry contacts) or transistorized outputs (current-sinking devices).

Override - A command extension available with some commands such as access point grant, access point group grant, and access point partition grant. When override is used with a grant command issued by a timed event, the access point opens for 30 seconds. When override is used as part of a grant issued via a keypad command (#77), the user is provided with prompts allowing a selection of door open time, alarm timeout, and prealarm time.

P

PIR (Passive InfraRed) - Typically, a sensor device that can sense movement within a specific area and change the state of a set of internal contacts as a result. These contacts can then be wired to a Request-to-Exit zone on an access control system for automated egress when a person approaches an access point from inside a protected area.

Pre-Alarm Trigger Time - This is the amount of time, in seconds, before the start of an access point door-open alarm, at which time the pre-alarm device is energized.

For example, if the door is set to be allowed to remain open for 30 seconds, an appropriate pre-alarm time is 10 seconds. After the door has been unlatched for 20 seconds, the system gives 10 seconds of warning to someone who is holding the door open. If the door is still open at the end of the 30 seconds, a door-open timeout alarm event occurs. The pre-alarm device will remain energized (depending upon its mode) until the door is closed, clearing the door-open timeout alarm.

Protected - The normal operating status of an Access Point. When an Access Point is protected, only valid cardholders can access it.

Proximity - A reader technology relying on a radio frequency link between the reader and the card (prox reader and prox card). Encoded information is passed between the card and reader, usually supplying a unique pattern enabling identification of the cardholder.

R

Reader - A device that a cardholder presents his access card to, that reads the card's encoded data and transmits it to an access control panel. The panel then makes a decision as to what action to take as a result of that card read (e.g., energize a relay, etc.).

RTE (Request-to-Exit) - A condition generated by a device other than a card reader (e.g., push-button, crash bar, PIR, switch floor mat) that indicates to the system that someone is leaving the protected area. No no forced door event is generated. It can also result in the door unlocking. Other names used in the industry for this condition are: REX, egress, and bypass.

NOTE: Do not confuse this usage of "bypass" with the ADEMCO meaning. (Please see Bypass)

S

Schedule (or Time Schedule) - A list of time intervals that can dictate when events or conditions can start, stop, or occur. For example, schedules control when certain access groups are allowed access to the premises. Schedules are made up of Day Templates.

Supervision - The process by which a device is monitored for faulty operation. This is typically accomplished through voltage or resistance monitoring. (Also see: EOLR Supervision and Relay Supervision)

T

Transaction - An event that occurred within the access control system which generates a record in the stored database.

Trigger Outputs - Solid-state digital switches (transistors) that can be configured as committed or uncommitted resources. These can be used to illuminate LEDs, activate piezoelectric sounders, energize an external relay, or signal a long-range radio transmitter.

Trouble - A condition that generally indicates a problematic line (cable or connection) for a supervised zone.

U

User Code - The identification code used by a user to gain access to the system. User codes are entered through the system interface.

APPENDIX B

Index

ADEMCO LIMITED WARRANTY

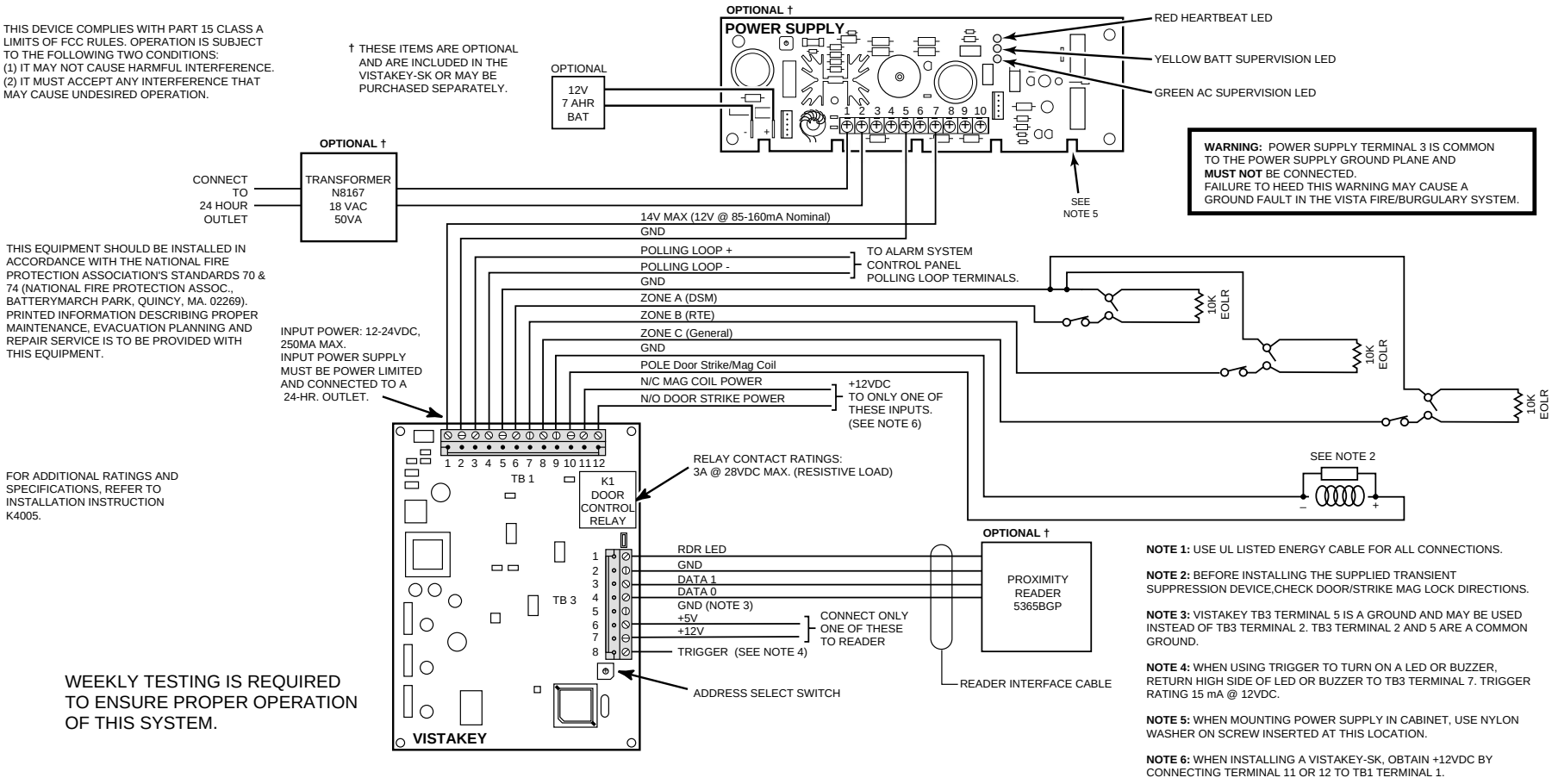
Alarm Device Manufacturing Company, a Division of Pittway Corporation, and its divisions, subsidiaries and affiliates ("Seller"), 165 Eileen Way, Syosset, New York 11791, warrants its products to be in conformance with its own plans and specifications and to be free from defects in materials and workmanship under normal use and service for 24 months from the date stamp control on the product or, for products not having an Ademco date stamp, for 12 months from date of original purchase unless the installation instructions or catalog sets forth a shorter period, in which case the shorter period shall apply. Seller's obligation shall be limited to repairing or replacing, at its option, free of charge for materials or labor, any product which is proved not in compliance with Seller's specifications or proves defective in materials or workmanship under normal use and service. Seller shall have no obligation under this Limited Warranty or otherwise if the product is altered or improperly repaired or serviced by anyone other than Ademco factory service. For warranty service, return product transportation prepaid, to Ademco Factory Service, 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 products it sells may not be compromised or circumvented; that the products will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the products will in all cases provide adequate warning or protection. Customer understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery, fire or other events occurring without providing an alarm, but it is not insurance or a guarantee that such will not occur or that there will be no personal injury or property loss as a result. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. HOWEVER, IF SELLER IS HELD LIABLE, WHETHER DIRECTLY OR INDIRECTLY, FOR ANY LOSS OR DAMAGE ARISING UNDER THIS LIMITED WARRANTY OR OTHERWISE, REGARDLESS OF CAUSE OR ORIGIN, SELLER'S MAXIMUM LIABILITY SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT, WHICH SHALL BE THE COMPLETE AND EXCLUSIVE REMEDY AGAINST SELLER. This warranty replaces any previous warranties and is the only warranty made by Seller on this product. No increase or alteration, written or verbal, of the obligations of this Limited Warranty is authorized.

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

† THESE ITEMS ARE OPTIONAL AND ARE INCLUDED IN THE VISTAKEY-SK OR MAY BE PURCHASED SEPARATELY.



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

FOR ADDITIONAL RATINGS AND SPECIFICATIONS, REFER TO INSTALLATION INSTRUCTION K4005.

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

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

NOTE 2: BEFORE INSTALLING THE SUPPLIED TRANSIENT SUPPRESSION DEVICE,CHECK DOOR/STRIKE MAG LOCK DIRECTIONS.

NOTE 3: VISTAKEY TB3 TERMINAL 5 IS A GROUND AND MAY BE USED INSTEAD OF TB3 TERMINAL 2. TB3 TERMINAL 2 AND 5 ARE A COMMON GROUND.

NOTE 4: WHEN USING TRIGGER TO TURN ON A LED OR BUZZER, RETURN HIGH SIDE OF LED OR BUZZER TO TB3 TERMINAL 7. TRIGGER RATING 15 mA @ 12VDC.

NOTE 5: WHEN MOUNTING POWER SUPPLY IN CABINET, USE NYLON WASHER ON SCREW INSERTED AT THIS LOCATION.

NOTE 6: WHEN INSTALLING A VISTAKEY-SK, OBTAIN +12VDC BY CONNECTING TERMINAL 11 OR 12 TO TB1 TERMINAL 1.

SUMMARY OF CONNECTIONS

165 Eileen Way, Syosset, New York 11791

K4005 6/00