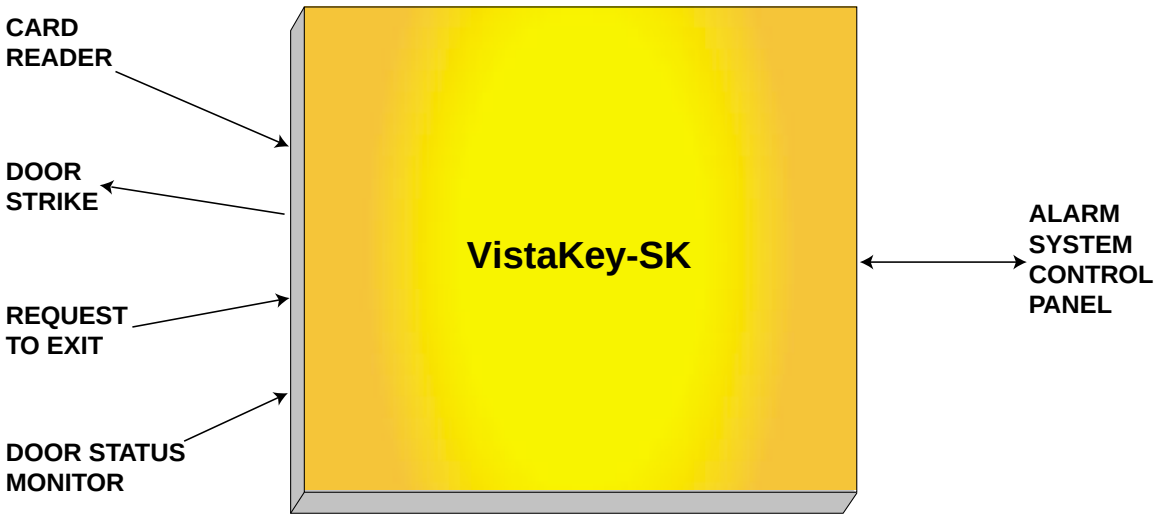
VistaKey-SK

Access Control Starter Kit

User Guide



K5398 6/00

ADEMCO

TABLE OF CONTENTS

Overview

Introduction

Congratulations on your ownership of a UL-approved ADEMCO VistaKey-SK Access Control Unit. The VistaKey-SK, interfaced to your security system, delivers a combination of access control capabilities with fire detection, intrusion detection, and hold-up systems. When connected to the control panel, the VistaKey-SK can operate the control panel and can provide access control to the protected premises.

The VistaKey-SK:

- Helps to reduce unwanted alarms caused by improper keypad operation by simplifying operation through the use of a card-swipe reader or wireless fob.
- Aids in reducing operational costs by eliminating the need to re-key caused by employee turnover.
- Helps to improve security by controlling access of individuals to specific areas in the protected premises.
- Assists in streamlining security operations by monitoring and recording user activity at a single location.
- Helps to minimize security investments by integrating access control, intrusion detection, and early-warning fire detection.

When the VistaKey-SK is interfaced to your security system, additional commands and operational capabilities are added to your system. This guide describes these additional commands and operational capabilities, and should be used with your existing security system User Guide.

The following commands are used to control access points, control cardholders, activate actions, create or modify time schedules, and create or modify time-driven events:

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
Schedule Control	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	#79	#80
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 may be used at a keypad 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 a time interval set by your system installer. 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 by your system installer.

Enter the #73 command as follows:

User Code + # + 73

The access point is unlatched for the time period defined by your system installer.

#74

The #74 command may be used to grant entry or exit through any access point. The access point will automatically relatch after a time interval set by your system installer. 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 they will be denied access while the partition is armed when 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 correspond to the access point number where entry or exit is to be allowed.

NOTE: 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

Press **0** for entry or **1** for exit. The access point is unlatched for the time period defined by your system installer.

#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 be 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 an assignment level of 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 they 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 correspond to the access point number where a change of state is desired.

NOTE: 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 defined by your system installer.

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 the [*] key 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*.

Output Device Control (#77)

The #77 Output Device Control may used to activate outputs, bypass zones, etc. under user control. The actions that may be activated by the user 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 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 1: Action Codes provides a listing of the "Action Codes" (desired actions) and describes their related specifiers.

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 prompt appears where you enter the specifier (i.e., relay number, partition number, etc.) for the action entered. Enter the specifier for the action selected.

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

```
↓ Action Number
01   Are You Sure?
 1=YES   0=NO          0
```

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

Press the [*] key to continue. The action specified (or cancellation) takes effect and the following message is displayed on the keypad:

```
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.

Schedule Control (#80)

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 *Performing Scheduling Operations*.

Table 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 (the XX value was set by the system installer)
05	Relay yy Sec	Relay #	Relay Close YY seconds – Close relay indicated by specifier for YY seconds (the YY value was set by the system installer)
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 (the XX value was set by the system installer)
10	Rly Grp yy Sec	Relay Group #	Relay Group Close YY seconds – Close relay group indicated by the specifier for YY seconds (the YY value was set by the system installer)
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)

Table 1: Action Codes (cont'd)

ACTION NO.	ACTION NAME	ACTION SPECIFIER	ACTION DESCRIPTION
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 bypasses the zone(s) specified on a particular zone list at the beginning of the window and unbypasses the zone(s) at the end of the window. If it is selected for auto unbypassing, the system removes the bypass of the zone(s) at the beginning of the window and restores the bypass 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
41	En Close Wind	Partition(s)	Enable Closing Window by partition – Enable the closing window for the partition indicated by the specifier
42	En Access Wind	Access Group	Enable Access Window for access group – Enable the access window for the access group indicated by the specifier (enables user arming or disarming)
50	Off-Normal Reminder	None	Off-Normal Reminder – Starts local keypad beeping if fire off-normal condition exists
Access Related Actions All access-related actions are active during the time window and you are not 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

Table 1: Action Codes (cont'd)

ACTION NO.	ACTION NAME	ACTION SPECIFIER	ACTION DESCRIPTION
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 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 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

Performing Access Control Card Functions

Access control card functions are performed using #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, provided near the end of this manual, and fill it in when assigning or re-assigning cards.

Keep the following advisories 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 Expired Use and Expire Month affect the life of a card given executive privileges. Also, cards programmed with executive privileges 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.
- 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 previously 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 are able to disarm partitions assigned to their access group. To prevent a card from accessing a door when the system is armed, the Armed Restriction must be set for the access goup. (Armed Restriction for an access group (if applicable) was set by your system installer.

Cards mapped to valid VISTA users in the system always have access to an access point and always can disarm a partition assigned to their access group in Access Group Programming. See the two examples below:

1. A card's access group was given access to a point by your system installer and Armed Restriction was not set. The following table illustrates the card's capabilities.

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 was given access to a point by your system installer and Armed Restriction was set. The following table illustrates the card's capabilities.

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 is displayed on the keypad:

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 system shows the "Add Card?" prompt. 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 as follows:

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 card or Edit a card by using a card swipe. Press **0** to advance to the Edit Card Function. When you press 1, the following prompt is displayed.

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

```
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 swiped has already been enrolled, the keypad sounds a double beep notifying you that the card has already been enrolled and that your entries will edit 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 responds in one of the following ways:

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 allows the cardholder to access any access point and disarm its partition (if armed) at any time.

This occurs 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 condition that prevents a cardholder with executive privilege from gaining access through an access point is a card that 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.

Press [*] to accept the entry.

NOTE: If 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.

↓ 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
```

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 assigned for the access group.

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

Press [*] to accept the entry.

NOTE: Numbers toggle. For example, pressing 1 turns group 1 on; 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 prevents entry grants even if the cardholder has executive privilege. Expiring a card does NOT delete it from the card database, and 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
07 = July	15 = End of Month

NOTES:

- Cards expire at midnight for month, end of day, end of week (Sunday), or 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 the day of the month. Note that the card expires at midnight of the day that you enter.

Press [*] to accept the entry.

↓ VISTA Card ID Number
001 Vista User#
000

Enter a three-digit VISTA User number.

The VISTA User number may be used to allow a cardholder access to an armed partition even if the cardholder's access group is restricted for that partition. Additionally, the VISTA User number 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 meanings:

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 1: Action Codes*.

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 where the display is dependent upon the action selected. For example, if the action you selected is **01** (relay on), the system presents a message asking for a relay number. Respond to the message presented, 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 is significantly different from one card to 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.

Press **1** to swipe additional cards with identical data definitions or **0** if additional cards with identical data definitions are not being entered.

```
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.

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
```

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

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

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

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

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

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.

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 allows the cardholder to access any access point and disarm its partition (if armed) at any time. This occurs 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 condition that prevents a cardholder with executive privilege from gaining access through an access point is a card that 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.

Press [*] to accept the entry.

NOTE: If 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.

↓ 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 assigned for the access group.

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

Press [*] to accept the entry.

NOTE: Numbers toggle. For example, pressing 1 turns group 1 on; 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 prevents entry grants even if the cardholder has executive privilege. Expiring a card does NOT delete it from the card database, and 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 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
07 = July	15 = End of Month

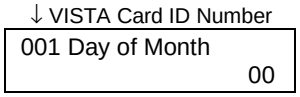
NOTES:

- Cards expire at midnight for month, end of day, end of week (Sunday), or 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.

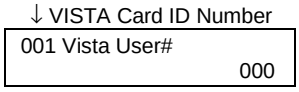
If you entered 01-12, the system displays the "Day of Month" prompt.

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



Enter the day of the month. Note that the card expires at midnight of the day that you enter.

Press [*] to accept the entry.



Enter a three-digit VISTA User number.

The VISTA User number may be used to allow a cardholder access to an armed partition even if the cardholder's access group is restricted for that partition. Additionally, the VISTA User number 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 meanings:

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 1: Action Codes*.

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 where the display is dependent upon the action selected. For example, if the action selected is **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 the "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 is displayed 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 as deleted in the card database.

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" number above, no cards are 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 selected cards as deleted in 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 the "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 as deleted in the card database and 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.

Time Windows

A time window is a period of time during which an event is permitted, or a specific time used to trigger an event. Note that time windows are optional and are not required to operate the system. They are only used to have time allow or cause an action. Time windows may be summarized as follows:

- Scheduled events are based on time windows, which are simply periods of time during which an event may take place.
- A time window is defined by a "Start" time and a "Stop" time.
- The system supports up to 20 time windows.
- The windows are shared by all partitions, and are used when programming time-driven events.

Preparing a Time Windows Worksheet

Fill out the Time Windows Worksheet (located near the end of this manual) using the steps outlined below.

NOTE: The time windows described here are also used to control other functions in your system. Your installer may have already programmed some time windows to control system functions. If some time windows have already been programmed, make certain that the first time window number you use is higher than the last number already programmed or you will overwrite your existing time windows.

As an aid to understanding the procedures for filling out the Time Windows Worksheet, assume that we want a time window that starts at 8:00 AM and ends at 5:00 PM and that this time window is number 1.

1. **Enter the Start Time desired for the time window. Note that if your system uses a 24-hour clock (i.e., 5:00 PM displays as 17:00) the time entered here must also be based on a 24-hour clock, so add 12 to any entries that are PM.**

Example: Enter 08:00 AM as the start time for time window 1.

Time Window Number	Start Time (HH:MM)	Stop Time (HH:MM)
1	***08:00 AM***	
2		

2. Enter the Stop Time desired for the time window. Note that if your system uses a 24-hour clock (i.e., 5:00 PM displays as 17:00) the time entered here must also be based on a 24-hour clock, so add 12 to any entries that are PM.

Example: Enter 05:00 PM as the stop time for time window 1.

Time Window Number	Start Time (HH:MM)	Stop Time (HH:MM)
1	*08:00 AM*	***05:00 PM***
2		

3. Repeat steps 1 and 2 for each time window desired.

When the worksheet entries have been completed, the time windows may be programmed into the system as described in the *Scheduling Menu Mode* paragraph later in this section. The Time-Driven Events Worksheet (if desired) may be completed before programming the time windows into the system.

Time-Driven Events

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.

These are the schedules used to activate outputs, bypass zones, etc. based on a time schedule. There are 20 events that may be programmed for the system, with each event governed by a previously defined time window.

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.

NOTES:

- The time-driven events described here are also used to control other functions in your system. Your installer may have already programmed some time-driven events to control system functions. If some time-driven events have already been programmed, make certain that the first Timed Event # you use is higher than the last number already programmed, or you will overwrite your existing time-driven events.
- 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.
- At the end of a time window controlling an access point, the access point will revert to the protect mode.

Preparing a Time-Driven Events Worksheet

Fill out the Time-Driven Events Worksheet (located near the end of this manual) using the steps outlined below.

As an aid to understanding the procedures for filling out the Time-Driven Events Worksheet, assume that we 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 to obtain this condition.

1. **Enter the Action No. listed in *Table 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 1: Action Codes* for the action number.

Example: Enter ACS Grp Enlb 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 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 (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 event/action is to occur within the Time Window specified. Note that when Holiday is selected, it will override 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).

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.

When you have completed the worksheet entries, program the time-driven events into your system as described in the *Scheduling Menu Mode* paragraph that follows.

Scheduling Menu Mode

The #80 Scheduling Menu Mode is used to program time windows and timed-event options. To enter this mode, the system must first be in the normal operating mode (all partitions disarmed).

The following can be programmed while in this mode:

- Time windows
- Open/close schedules*
- Holiday schedules*
- Timed events
- Access schedules*

*** IMPORTANT:** The schedule options denoted by the * should not be used. Your system installer programmed these items, if applicable.

To program schedules, enter the Scheduling Program Mode:

User Code + # + 80.

NOTE: This mode can only be entered when all partitions are disarmed.

There are 5 sections of scheduling menus, as shown below. Pressing **1** at a displayed main menu prompt selects that menu option. Prompts for programming that option then appear. Press **0** to skip a section and display the next menu option.

Time Window ?
1 Yes 0 = No 0

Upon entering Schedule Menu Mode, this prompt appears. Press **1** to program time windows. Refer to *Time Windows Programming* later in this section for detailed instructions.

Press **0** to move to the "O/C Schedules?" prompt.

O/C Schedules ? 1 Yes 0 = No 0

Press **1** to program opening and closing schedules.

IMPORTANT: This schedule option should not be used. Your system installer programmed this item, if applicable.

Press **0** to move to the "Holidays?" prompt.

Holidays ? 1 Yes 0 = No 0

Press **1** to program holiday schedules.

IMPORTANT: This schedule option should not be used. Your system installer programmed this item, if applicable.

Press **0** to move to the "Timed Events?" prompt.

Timed Events ? 1 Yes 0 = No 0

Press **1** to program timed events for relay outputs, additional schedules, and other system functions. Refer to *Time-Driven Event Programming* later in this section for detailed instructions.

Press **0** to move to the "Access Sched?" prompt.

Access Sched. ? 1 Yes 0 = No 0

Press **1** to program access schedules.
IMPORTANT: This schedule option should not be used. Your system installer programmed this item, if applicable.

Press **0** to move to the "Quit?" prompt.

Quit ? 1 Yes 0 = No 0

Press **1** to quit *#80 Scheduling Menu Mode* and return to normal operating mode.

Press **0** to make any changes or review the scheduling programming options. If you press **0**, the "Time Window?" prompt is displayed.

Time Windows Programming

Enter Scheduling Mode by entering **User Code + [#] + 80** if you are not already in the Scheduling mode. The keypad displays the "Time Windows?" programming prompt.

```
Time Windows  ?
1 Yes   0 = No            0
```

Press **1** at this main menu prompt to program time windows.

```
TIME WINDOW # ?
01-20,  00 = QUIT        01
```

Enter the 2-digit time window number **(01-20)** to be programmed.

Press [∗] to accept the entry.

Enter **00 + [∗]** at the "TIME WINDOW #?" prompt to quit time window programming and display the "Quit ?" prompt.

```
01  TIME WINDOW
00:00AM          00:00AM
```

If you entered a time window number, the cursor is now positioned on the starting hour of the time window.

Enter the desired starting hour and press [∗]. The cursor moves to the minutes position. Enter the desired minutes and press [∗]. Toggle the AM/PM indication by pressing any key 0-9 while the cursor is under the A/P position and then press [*]. Repeat this to enter the stop time of the window.

Note that if your system uses a 24-hour clock (i.e., 5:00 PM displays as 17:00) the time entered here must also be based on a 24-hour clock so add 12 to any entries that are PM.

When the entry is completed, the "TIME WINDOW #?" prompt is displayed again.

Enter the next time window number to be programmed and repeat the procedure; or enter 00 and press [*] to quit programming time windows. When you enter 00*, the keypad displays the following:

Quit ?
1 = yes 0 = no 0

Press **0** at the "Quit ?" prompt to return to the main menu choices and continue programming.

Press **1** to quit Scheduling Menu Mode.

NOTE: Because the time windows are shared among all partitions, it is important to make sure that changing a time window does not adversely affect other programmed Time-Driven events.

Time-Driven Event Programming

The following schedules can be used to activate outputs, bypass zones, arm/disarm the system, etc. based on a time schedule. Up to 20 events can be programmed for the system. Time windows must first be defined in order to be used to trigger events.

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

Timed Events ?
1 yes 0 = no 0

Press **1** to program timed events.

TIMED EVENT # ?
01-20, 00=QUIT 01

Enter the timed event number to be programmed **(01-20)**.

Press [*].

The system prompts you to enter the desired action to be taken.

Enter **00** at the "TIMED EVENT #?" prompt to quit the timed event menus and display the "Quit ?" prompt.

01 ACTION ?
none 00

Enter the action code for this timed-event number from your Time-Driven Events Worksheet.

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 [∗] to accept the entry. The prompt for the action specifier will display.

Action Specifier:

Actions 01-05

01 RELAY # ?
00

If you selected actions **01-05**, the prompt at the right is displayed. Enter the relay number.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

Actions 06-10

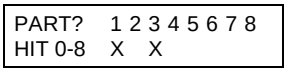
01 RELAY GRP # ?
00

If you selected actions **06-10**, the prompt at the right is displayed. Enter the relay group number.

Press [∗] to accept entry.

The "Time Window ?" prompt appears.

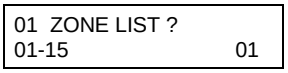
Actions 21-24, 40-41, and 67-72



If you selected actions **21-24, 40-41,** or **67-72**, the prompt at the right is displayed. Enter the partition to which the action applies. Press **0** to toggle all partitions on or off; or press keys **1**-**8** to toggle the letter "x" under the partition numbers to turn them on or off.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

Actions 30-31



If you selected actions **30-31**, the prompt at the right is displayed. Enter the zone list number that contains the zones to be bypassed or unbypassed.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

Action 42

```
GROUP? 1 2 3 4 5 6 7 8
HIT 0-8                X
```

If you selected action **42**, the prompt at the right is displayed. Press **0** to toggle all groups on or off; or press keys **1-8** to toggle the letter "x" under the group numbers to turn them on or off.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

Actions 55-60

```
ACCESS POINT #?
00-31                  00
```

If you selected actions **55-60**, the prompt at the right is displayed. Enter the access point number (from 01 through 15).

Press [∗] to accept entry. The "Time Window ?" prompt appears.

Actions 61-66 and 77-78

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

If you selected actions **61-66** or **77-78**, the prompt at the right is displayed. Enter the group number to which the access action applies. 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 to turn them on or off.

Press [∗] to accept entry. The "Time Window ?" prompt appears.

```
01 Time Window ?
00:00  00:00        01
```

Enter the time window number (**01-20**) for which this timed event is to occur. As the number is keyed in, the actual time that has been stored for the time window number is displayed.

Press [∗] to accept entry.

```
01 Active time ?
                    0
```

Enter the activation time from **1-4** (listed below). As the number is keyed in, the activation time is displayed. The choices are:

- **1:** Trigger at the start of the window.
- **2:** Trigger at the end of the window.
- **3:** Take effect only for the duration of the window.
- **4:** Trigger at both the start and the end of the window.

Press [∗] to accept entry.

```
Days ?  MTWTFSSH
Hit 0-8  x  x
```

The system then asks for which days the event is to be activated.

Press **0** to toggle all days on or off; or else press keys **1-8** to toggle the letter "x" under the days to turn them on or off (Monday = 1, Holiday = H = 8).

NOTE: When holiday is selected, it will override 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).

When all entries have been made, the "TIMED EVENT #?" prompt is displayed again.

Repeat the procedure for each timed event required for the installation.

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

Press **0** at the "Quit ?" prompt to return to the main menu choices and continue programming. Press **1** to quit Scheduling Menu Mode.

Reduced Capability Mode

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.

NOTE: 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.

Reduced Capability Mode (cont'd)

- 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.

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	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						
		Y N	Y N	1234 5678						

Time Window Worksheet

Time Window Number	Start Time (HH:MM)	Stop Time (HH:MM)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

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													

Index

ADEMCO ONE YEAR 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 security equipment (the "product") to be free from defects in materials and workmanship for one year from date of original purchase, under normal use and service. Seller's obligation is limited to repairing or replacing, at its option, free of charge for parts, labor, or transportation, any product proven to be defective in materials or workmanship under normal use and service. Seller shall have no obligation under this warranty or otherwise if the product is altered or improperly repaired or serviced by anyone other than the Seller. In case of defect, contact the security professional who installed and maintains your security equipment or the Seller for product repair.

This one year Limited Warranty is in lieu of all other express warranties, obligations or liabilities. THERE ARE NO EXPRESS WARRANTIES, WHICH EXTEND BEYOND THE FACE HEREOF. ANY IMPLIED WARRANTIES, OBLIGATIONS OR LIABILITIES MADE BY SELLER IN CONNECTION WITH THIS PRODUCT, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, ARE LIMITED IN DURATION TO A PERIOD OF ONE YEAR FROM THE DATE OF ORIGINAL PURCHASE. ANY ACTION FOR BREACH OF ANY WARRANTY, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, MUST BE BROUGHT WITHIN 12 MONTHS FROM DATE OF ORIGINAL PURCHASE. 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. Some states do not allow limitation on how long an implied warranty lasts or the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Seller does not represent that the product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. Buyer 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 gives you specific legal rights, and you may also have other rights which vary from state to state. No increase or alteration, written or verbal, to this warranty is authorized.

ADEMCO GROUP

165 Eileen Way, Syosset, New York 11791

K5398 6/00