

# PassPoint *Express*

---

## USER GUIDE

---

*For Access Control Kits*

**ADEMCO**  
**GROUP**

K3298 5/98

### **IMPORTANT NOTICE**

This product complies with Standards of UL294 only. It has not been tested for compliance with Standards of UL1076. The burglary features of this product are only supplemental to the product's access control features. Terms used in this documentation, such as zones, perimeter, etc., are not indicative of UL approved burglary features. These terms apply only to access control applications of this product and the product's burglary features that have not been approved by UL.

## ALARM DEVICE MANUFACTURING COMPANY

A Division of Pittway Corporation  
165 Eileen Way, Syosset, NY 11791

### SOFTWARE LICENSE AGREEMENT

**You should carefully read the following terms and conditions. BY BREAKING THE SEAL ON THIS PACKAGE YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. If you do not consent to be bound by this License Agreement, you must promptly return the unopened package to the person from whom you purchased it within fifteen (15) days from date of purchase and your money will be refunded to you by that person. If the person from whom you purchased this Software fails to refund your money, contact ADEMCO immediately at the address set out above.**

1. **GRANT OF LICENSE.** Subject to all terms and conditions hereof, Alarm Device Manufacturing Company, a division of Pittway Corporation ("ADEMCO") does hereby grant to the purchaser (the "Licensee") upon payment in full of the published license fee, or other license fee agreed to in writing (the "License Fee") a nontransferable, nonexclusive license to use the enclosed software ("Licensed Programs") provided herewith in Licensee's own business on a single computer for a term commencing on the date of payment in full of the License Fee and continuing in perpetuity unless terminated in accordance with the terms hereof.
2. **PROPRIETARY RIGHTS.** Licensee hereby acknowledges that the Licensed Programs including the algorithms contained therein are proprietary to ADEMCO. Licensee shall not sell, transfer, disclose, display or otherwise make available any Licensed Programs or copies or portions thereof to any other entity. Licensee agrees to secure and protect the Licensed Programs so as to maintain the proprietary rights of ADEMCO therein, including appropriate instructions to and agreements with its employees.
3. **DOCUMENTATION.** The documentation supplied with the Licensed Programs is the copyright property of ADEMCO. Licensee shall not under any circumstances divulge or permit to be divulged such documentation to any other entity.
4. **COPIES.** Licensee shall not copy in whole or in part the Licensed Programs or documentation provided however that Licensee shall be permitted to make one (1) copy of the Licensed Programs solely for backup purposes provided that all proprietary notices are reproduced thereon. Any such copy shall remain part of the Licensed Programs and shall be subject to this Agreement.
5. **OBJECT CODE.** Licensee understands and acknowledges that the Licensed Programs consist of object code only and that ADEMCO shall not supply source code versions of the Licensed Programs. Licensee shall not create or attempt to create by de-compilation or otherwise, the source code for the Licensed Programs, or any part thereof.
6. **SECURITY.** Licensee acknowledges that the Licensed Programs are security related and access to the Licensed Software should be limited to authorized individuals. Licensee assumes full responsibility for use of the Licensed Programs whether by authorized or unauthorized individuals. Licensee agrees that the License Fee has been set in reliance upon indemnities and the limitations on liability contained herein and that such provisions are fair and not unconscionable.
7. **LIMITED WARRANTY.** ADEMCO warrants that the Licensed Programs will conform to the functions described in the ADEMCO user documentation provided herewith for ninety (90) days from the date of original purchase. THE WARRANTY STATED ABOVE IS A LIMITED WARRANTY AND IT IS THE ONLY WARRANTY BY ADEMCO. ALL OTHER WARRANTIES OF MERCHANTABILITY OR WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED BY ADEMCO AND WAIVED BY LICENSEE. Other than the limited warranty stated above, the entire risk as to the use, quality and performance of the Licensed Programs is with Licensee. ADEMCO does not represent that the Licensed Programs may not be compromised or circumvented; that the Licensed Programs will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the Licensed Programs will in all cases provide adequate warning or protection. Licensee understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery or fire without warning, but 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. ADEMCO does not warrant that the Licensed Programs will meet Licensee's

requirements or that the operation of the Licensed Programs will be uninterrupted or error free. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

8. LIMITATION OF REMEDIES. Licensee's exclusive remedy shall be either the replacement of any diskette not meeting the limited warranty set forth above and which is returned to ADEMCO with a copy of Licensee's paid invoice or, if ADEMCO is unable to deliver a replacement diskette which is free of defects, Licensee may terminate this Agreement by returning the Licensed Programs and thereupon the License Fee shall be refunded. ADEMCO shall have no obligation under this Limited Warranty if the Licensed Programs are altered or improperly repaired or serviced by anyone other than ADEMCO factory service. For warranty service, return Licensed Programs transportation prepaid, to ADEMCO Factory Service, 165 Eileen Way, Syosset, NY 11791. ADEMCO SHALL HAVE NO LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR WITH RESPECT TO AUTHORIZED OR UNAUTHORIZED USE OF THE LICENSED PROGRAMS OR OTHERWISE WHETHER BASED IN CONTRACT, TORT OR UPON ANY OTHER LEGAL THEORY FOR CONSEQUENTIAL EXEMPLARY, OR INCIDENTAL DAMAGES, INCLUDING BUT NOT LIMITED TO LIABILITY FOR PERSONAL INJURY, PROPERTY DAMAGE, ECONOMIC LOSS, OR CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS OF LICENSEE, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall ADEMCO's liability whether direct or indirect for any claim, under this Agreement or otherwise, regardless of cause or origin, exceed the License Fee. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSIONS OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

9. REGISTRATION. In order to qualify to receive notification of ADEMCO updates to the Licensed Programs, Licensee must complete and return the enclosed Registration Form to ADEMCO within twenty (20) days from date of purchase. Notwithstanding, ADEMCO is under no obligation to release updates to the Licensed Programs.

10. TERMINATION. Upon the breach or non-compliance with any term or provision of this Agreement, ADEMCO shall have the right to terminate the license granted hereby by written notice to Licensee. Upon such termination Licensee shall immediately turn over to ADEMCO all copies of the Licensed Programs and any documentation supplied in connection therewith. Such remedy shall be in addition to and cumulative to any other remedies ADEMCO may have at law or in equity with respect to such breach or non-compliance.

11. GENERAL. This agreement is the complete and exclusive statement of the understanding of the parties involved with respect to the transaction contemplated hereby and supersedes any and all prior proposals, understandings and agreements. This Agreement may not be modified or altered except by a written instrument signed by Licensee and an authorized representative of ADEMCO. Licensee may not assign or sublicense without the prior written consent of ADEMCO, its rights, duties or obligations under this Agreement to any person or entity, in whole or in part. If any provision of this Agreement is invalid under any applicable statute or rule of law it is to that extent to be deemed omitted. This Agreement and the performance hereunder shall be governed by the laws of the State of New York and the sole venue for suit shall be in an appropriate state or federal court located in the State and City of New York. The failure of ADEMCO to exercise in any respect any rights provided for herein shall not be deemed a waiver of such right or any further right hereunder. No action regardless of form arising in connection with this Agreement may be brought more than two (2) years after the date such cause of action shall have arisen. ADEMCO shall have the right to collect from Licensee any expenses incurred including attorneys' fees in enforcing its right under this Agreement.

# Table of Contents

<b>Introduction.....</b>	<b>1-1</b>
About This Guide.....	1-2
What Is PassPoint Express? .....	1-3
Starting Express .....	1-5
The PassPoint Express Environment .....	1-5
<b>User Levels.....</b>	<b>2-1</b>
Understanding User Levels.....	2-2
User Level Permissions .....	2-5
Assigning User Codes.....	2-8
<b>Managing Cards and the Cardholder Database .....</b>	<b>3-1</b>
About the Cardholder Database .....	3-2
Using the Card Wizard .....	3-4
Adding Cards Manually .....	3-10
Using the Action tab .....	3-16
<b>Setting Administration Options.....</b>	<b>4-1</b>
PassPoint Administration Options .....	4-2
Administration dialog box fields .....	4-3

<b>Access Groups .....</b>	<b>5-1</b>
What Are Access Groups? .....	5-2
Creating Access Groups and setting attributes .....	5-3
Assigning schedules to an Access Group .....	5-6
Assigning Access Points to an Access Group .....	5-8
Disabling and Enabling Access Groups.....	5-9
Entry/Exit Control.....	5-10
Configuring Entry/Exit control.....	5-12
<b>Time Scheduling.....</b>	<b>6-1</b>
What Is PassPoint Scheduling?.....	6-2
Set the MLB Time .....	6-4
Day Templates .....	6-4
Creating Day Templates .....	6-7
Holidays .....	6-9
Assigning holidays.....	6-11
Time Schedules.....	6-12
Creating Schedules .....	6-15
Resynchronizing Schedules .....	6-20
<b>Event-Action Relationships.....</b>	<b>7-1</b>
What Are Event-Action Relationships?.....	7-2
Creating event-action relationships .....	7-3
<b>Precedence Levels .....</b>	<b>8-1</b>
What is Precedence? .....	8-2
Using precedence .....	8-5
Precedence level scenarios.....	8-6
<b>The Event Log .....</b>	<b>9-1</b>
What Is the Event Log? .....	9-2
The Event Browser .....	9-3

---

<b>Setting System-Wide Options .....</b>	<b>10-1</b>
PassPoint System-Wide Options .....	10-2
System presets.....	10-4
Card technology options .....	10-7
Skeleton codes .....	10-9
Burglary system options .....	10-13
Access point beeps and video .....	10-16
Dialer reporting options .....	10-17
Modem options .....	10-17
Network ID options .....	10-20
Priority options .....	10-23
<b>Performing Access Functions.....</b>	<b>11-1</b>
What Are Access Point Functions? .....	11-2
Displaying and controlling Access Points .....	11-3
Locking Access Points.....	11-5
Protecting Access Points.....	11-5
Bypassing Access Points .....	11-6
Granting access to Access Points.....	11-7
Shunting and unshunting Access Points .....	11-10
Choosing an identification method .....	11-10
Setting Access Points as Exit Only.....	11-12
Configuring Visual Identification.....	11-13
Clearing the precedence level of an Access Point .....	11-14
Anti-Passback .....	11-15
Configuring Anti-Passback.....	11-17
Forgiving Anti-Passback.....	11-17
Threat Levels .....	11-19
<b>Uploading and Downloading the Database .....</b>	<b>12-1</b>
What Is the Database?.....	12-2
System accounts.....	12-2
What information is in the account database? .....	12-3
Downloading the database .....	12-4
Uploading the database.....	12-5

---

---

<b>Using PassPoint Reports .....</b>	<b>13-1</b>
PassPoint Reporting .....	13-2
Using the Event Reporter .....	13-4
Viewing reports .....	13-6
<b>System Defaults .....</b>	<b>A-1</b>
<b>Keypad Messages .....</b>	<b>B-1</b>
<b>Event Log Messages .....</b>	<b>C-1</b>



## Chapter

# 1

## *Introduction*

This chapter describes the content of this guide and explains the basic use of the PassPoint Express program. In this chapter you will learn:

- **What this guide is about and what its contents are**
- **What the PassPoint Express Windows software is and how to use it.**

## ***About This Guide***

This guide is for users of the PassPoint access control system. It contains everything needed to operate the system on a day to day basis once the system has been installed and properly configured.

### ***Who is a user?***

A *user* of the system is a person that interacts with the system through its interface. Users can control readers, set time schedules, enroll ID cards, etc.

Users interact with the system on a completely different level from Cardholders. Cardholders are the people who occupy the premises. They have nothing to do with the configuring or operation of the system. A user will most likely be a Cardholder, but a Cardholder does not have to be a system user.

For example, the security manager posted of a premises with PassPoint is both a Cardholder and a PassPoint user. He is a Cardholder because he has an access badge to allow him access to the premises. He is also a system user because he is responsible for configuring and operating the PassPoint system. He sets up time schedules, enrolls new ID cards, etc.

There are four different levels of PassPoint users. They are: Installer, Masters, Managers, and Operators. Each of these user levels are explained in detail in the following chapter of this guide.

### ***What's in this guide?***

All of the tasks that a system user performs are described in this guide.

When using the system, you will be working with the PassPoint Express system interface. This system interface allows you to

perform all of the tasks needed to configure, monitor, and operate your PassPoint system.

## ***What Is PassPoint Express?***

PassPoint Express is a Windows 95 software program that installs and runs your system terminal. Essentially, PassPoint *Express* allows your PC to communicate with the main logic board of the system.

With PassPoint *Express*, you can configure all of the options necessary to get your system up and running, perform system maintenance, and monitor system functioning. While monitoring the system, PassPoint *Express* displays a scrolling list of system events. A user can then log on and enter the program's visually oriented system, which allows full screen editing of configurable options.



---

The PassPoint system does not need to be connected to the PassPoint *Express* PC in order to function. The PC is only used to configure and monitor the system. Once the system is up and running, the PC can be disconnected (either intentionally or unintentionally) without disrupting the operation of the system.

---

## ***System requirements***

In order to install and run PassPoint *Express*, your PC will need to have the following minimum configuration:

### **Minimum**

- **P90 Class processor**
- **16 megabytes RAM**
- **20MB free hard disk space**
- **Windows 95**
- **SVGA video display, 800x600 resolution, 256 color**
- **Mouse**
- **1 available serial port for MLB**

### **Optional**

- **1 available serial port for TWAIN digital camera (optional)**
- **TWAIN compliant scanner (optional)**
- **2 Hayes-compatible 28.8 modems (optional for remote operation)**
- **Integral Flashpoint Lite or better (optional for on-screen video)**

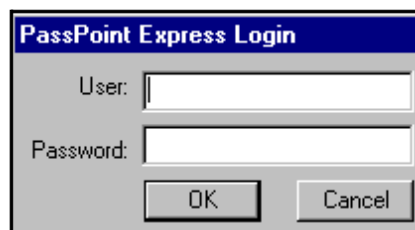
## Starting Express

To start Express on your PC:

To start PassPoint *Express* on your PC:

1. **Select *PassPoint Express* from the Windows 95 Program menu.**

In a few moments, the system will prompt you for a user name and password:



2. **Enter your user name and password and click *OK*.**

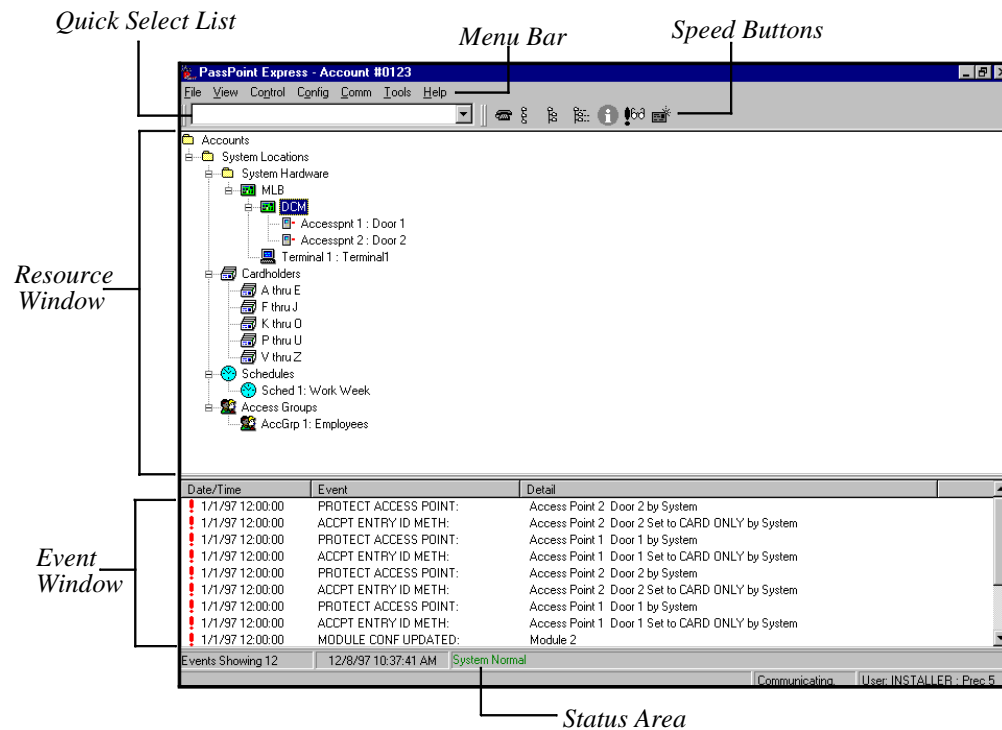
Once you click *OK*, the main *Express* window appears on your screen.

## The PassPoint Express Environment

PassPoint *Express* has been designed to be simple to use. If you are already familiar with operating in a Windows environment, you should have no trouble finding your way around the PassPoint *Express* screen.

## Major screen components

The illustration below shows the main PassPoint *Express* screen as it would look if the system were fully up and running. This is, it includes card holders, time schedules, etc.



**Resource Window** - All of your system resources are listed in the Resource Window. Resources can be modules (like MLBs or DCMs), relays, zones, triggers, etc. Certain objects in the Resource Window can be controlled by right-clicking on them.

**Event Window** - Each time a new system event occurs, it appears in the Event Window. Examples of system events are bypassing a zone, enabling a relay, disabling a card reader, etc. The most recent event appears at the top of the list in the Event Window.

**Menu Bar** - The menu bar allows you to select commands for the operation of the program.

**Quick Select List** - The Quick Select List lists all of your system's components and resources. Use the list to quickly locate the system objects you are looking for.

**Speed Button Bar** - Like the menu bar, the speed button bar allows you to select commands for program operation. Each speed-button function has a corresponding menu command on the menu bar.

**Status Area** - The Status Area provides information about the current operating conditions of your PassPoint system. Whenever an important system event or trouble occurs, a message indicating the event will appear here in red. In the illustration on the previous page, we can see that three important system events are in progress: a system module is failing communication, an Access Point is locked, and a zone is bypassed.





Chapter

# 2

## *User Levels*

This chapter explains how to use PassPoint user access codes. In this chapter you will learn:

- **What the four PassPoint user levels are and how they are used**
- **About the different level of system access provided by each user level**
- **How to assign user codes**

## ***Understanding User Levels***

A *User* of the system is a person who interacts with the system through one of its interfaces. Users interact with the system on a completely different level from occupants. Remember that occupants are Cardholders. These are the people who occupy the premises. They have nothing to do with configuring the system's day-to-day operation. This is the job of users.

There are four categories, or levels, of users. Each level has a different degree of access to the system. The four user levels are:

- **Installers**
- **Masters**
- **Managers**
- **Operators**

### ***Installers***

The system supports **one** installer-level user.

The installer is the only user who is allowed to alter the hardware configuration of the system. That is, he/she is the only person who can determine which doors, zones, readers, relays and such are used by the system.

The installer can also arm and disarm the burglary features of PassPoint, as well as control all access points (i.e., bypassing and locking) and general resources (i.e., output relays and triggers). If the installer arms the system, any other user can

disarm it. The installer cannot disarm the system once it has been armed by another user.

Lastly, the installer can modify the occupant card database and view the event log.

### **Masters**

The system supports **four** master-level users.

While the Installer is the highest-authority user of the system, a Master is intended to be the highest-authority user of the system who remains on premises.

A system master can perform all access control and burglary protection features as well as control uncommitted resources (i.e., system resources not associated with access points). The system master can also perform occupant card database management functions.

Since the system master is the highest-capability user on the premises, the master will most likely be the “chief of security.”

### **Managers**

The system supports **eight** manager-level users.

A system manager can not perform access control or burglary related control functions. A system manager can perform occupant card database management functions and perform event log and data extraction functions.

Managers will most likely be comprised of Human Resources or Accounting personnel. A manager’s interaction with the

system will primarily consist of card database maintenance or accounting data extraction.

### ***Operators***

The system supports **eight** operator-level users.

The operator user level is intended to be assigned to guards. When a user terminal is installed at an entry point manned by a guard, the guard can interact with PassPoint in order to visually verify an occupant's identity before allowing entry. If the entry point is programmed for visual verification, upon the occupant's swipe, the guard will be prompted with the occupant's name. The guard must then indicate if the occupant's identity is correct before PassPoint will allow the door to open.

An operator can perform access control and burglary-related functions. An operator cannot alter the occupant card database.

### ***Every user has an access code***

Each user of the system, whether an installer, master, manager or operator, is given an access code. This is the code the user uses to log-in to the system. You have already seen how to log-in using your default installer code.

In this chapter you will be seeing how to change your default installer code, as well as how to assign codes to the other users of your system.

## User Level Permissions

In order to help you understand the four user levels, the following table lists each of the tasks available to each user level from the menus of the *Express* system interface.

Function	Installer	Master	Manager	Operator
<b>Hardware Configuration</b>				
Set security ANET node number	<input type="radio"/>			
Configure access ANET nodes	<input type="radio"/>			
Access area configuration	<input type="radio"/>			
Reader configuration	<input type="radio"/>			
Relay configuration	<input type="radio"/>			
Zone configuration	<input type="radio"/>			
Access area/reader/relay/zone name editing	<input type="radio"/>			
Default all configuration options	<input type="radio"/>			
Edit relay, zone, reader, trigger & script names	<input type="radio"/>			
<b>User Code Related Functions</b>				
Edit installer code	<input type="radio"/>			
Add/Edit/Delete master codes	<input type="radio"/>	Only his/her own code		

Function	Installer	Master	Manager	Operator
Add/Edit/Delete manager codes	<input type="radio"/>	<input type="radio"/>	Only Manager codes	
Add/Edit/Delete operator codes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Can only change his/her own password
Edit manager's privilege assignment capability				
<b>Access Card/Access Code Related Functions</b>				
Add cards/codes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Edit cards/codes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Delete cards/codes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
View cards/codes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Edit access groups	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Edit access group privileges	<input type="radio"/>	<input type="radio"/>		
<b>Event Logging Functions</b>				
Select which events are logged	<input type="radio"/>			
Set dialer characteristics	<input type="radio"/>			
Select which events cause dialer reports	<input type="radio"/>			

Function	Installer	Master	Manager	Operator
<b>Scheduling Functions</b>				
Edit holidays	<input type="radio"/>	<input type="radio"/>		
Edit time windows	<input type="radio"/>	<input type="radio"/>		
Edit schedules	<input type="radio"/>	<input type="radio"/>		
Set the time	<input type="radio"/>	<input type="radio"/>		
Assign script/action to schedules	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Edit event-action relationships	<input type="radio"/>	<input type="radio"/>		
<b>Access Control Related Functions</b>				
Protect access points	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Bypass access points	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Lock access points	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Turn visual verification on/off at access points	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Visually verify card/code holders in order to grant access		<input type="radio"/>		<input type="radio"/>
<b>Security Functions</b>				
Arm/Disarm burglary zones	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Bypass/Protect burglary zones	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>

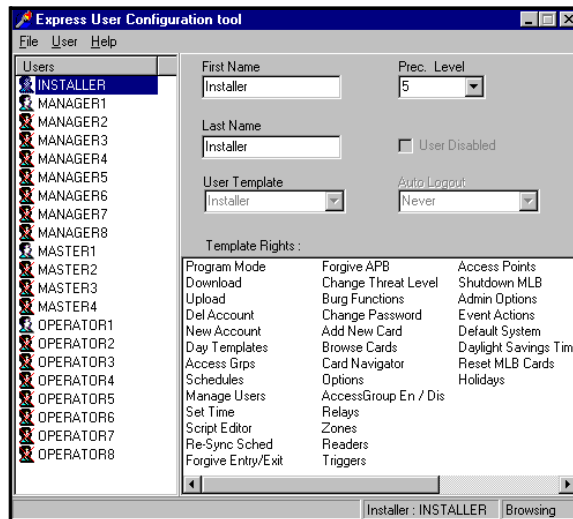
Function	Installer	Master	Manager	Operator
Reset latching glassbreaks	<input type="radio"/>			
<b>Uncommitted Resource Functions</b>				
Enable/Disable uncommitted readers	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Enable/Disable uncommitted relays	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Toggle relays	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
<b>Other Functions</b>				
View module communication fault status	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
View relay supervision status	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
View AC loss/low battery status	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## ***Assigning User Codes***

All PassPoint user codes are assigned the same way, using a dedicated dialog box that lists all the current user codes for the system.



To reach this dialog box, select *Manage Users* from the *Tools* menu:



This dialog box allows the names of the users to be configured and displays each user's privileges. Note that since there are varying levels of log-in authority, any user using this dialog box can change only their own properties or properties of users at a lower privilege level.

This dialog box has two panes. The left pane lists the log-in users and the right pane displays the details about a selected user.

The dialog box also displays a status bar along the bottom. The two right-most panes of the status bar display the current user being displayed and whether any edits have taken place. If no edits have been performed on the selected user, the right-most status pane will display "Browsing." Once an edit has been performed that has not been saved, this pane will display

“Editing.” In order to save any edits, use the *User...Save Changes* menu command or click on a different user in the User list.

***Users List***

Click a user in this list in order to update the detail display on the right side of this screen.

***Fields***

**First Name** - You can edit the first name of each user in this text box.

**Last Name** - You can edit the last name of each user in this text box.

**User Disabled** - Click this list box if you want to temporarily disable a user’s access.

**Prec. Level** - Select this drop-down list so that you can choose the precedence level of each user. Remember that precedence levels define which users have authority over other users, schedules, cardholders, and actions.

**User Template** - This field will indicate the type of user that is being edited.

***Template Rights***

This list will display the capabilities of the selected user. These capabilities are defined by the User Template and cannot be changed.

## **Menu commands**

### **File Menu**

Select *Exit* from the file menu when you have finished editing user data.

### **User Menu**

**Reset Password** – Use the Reset Password menu command when you want to set a user’s password back to its default. Doing this will set the password back to INSTALLER, MASTERx, MANAGERx, or OPERATORx (with x being the number of the log-in).

**Save Changes** – Use the *Save Changes* menu command when you want to save your edits without exiting the User Configuration Tool.

### **Help Menu**

Opens up the Help system and shows system revision information.



Chapter

3

## *Managing Cards and the Cardholder Database*

In this chapter you will learn how to:

- **Use the Cardholder database**
- **Use the Card Wizard to add a single card or a batch of cards**
- **Add a card to the database manually**
- **Associate an action with a card**

---

## About the Cardholder Database

In order to keep track of all of its Cardholders, PassPoint uses a database. The PassPoint Cardholder database contains the names of all of the Cardholders of the premises. It associates each Cardholder with his/her ID card's code, as well as the Cardholder's Personal Identification Number (PIN). It is here, in the Cardholder database, that you assign cards and PINs to Cardholders.

### ***Adding Cardholders to the system***

Each time you want to issue a card, you are adding a Cardholder to the database. In addition to the Cardholder's name, ID card and PIN, you can enter such information as the Cardholder's Access Group assignments, the type of card he/she is using, etc. Some of this information is mandatory to enter. Other information is optional and is intended to make locating and managing Cardholders easier.

*For example, Cardholders can be assigned to up to five different Access Groups, but they must be assigned to at least one. Otherwise, they will never be able to access any of your premises' Access Points.*

Also, each Cardholder card can be assigned to invoke a specific system action. The action can be set to initiate under a variety of circumstances, such as an access grant, an access denial, or an egress grant.

Cards can be assigned to Cardholders on a temporary basis, allowing an expiration date or usage count to determine the period throughout which the card will be valid.

*For example, if you want to give a card to a visitor for only one day, you can set the card to expire on the following day. Or, if you want the card to only work for three entries into your building, you can set the card to deny every entry request after the third.*

**Where do you start?**

There are two main ways to enroll a card. One is to use the Card Wizard. The other is to use the *Add New Card* function. Both methods are explained below:

- **The Add New Card function**

This function is chosen from the *Config* menu, and brings up a dialog box that allows you to fill in the data for the card manually.

Adding a card with the *Add New Card* function allows you the greatest flexibility. The Card dialog box contains a number of fields that can be edited and tailored for the particular Cardholder.

The *Add New Card* function allows you to add only one card. If you want to add more than one card, use the Card Wizard.

- **The Card Wizard**

The Card Wizard is a PassPoint tool that lets you enroll cards quickly and easily. Using the Card Wizard, you can enroll a single card, or you can enroll a batch of cards.

Adding a card using the Card Wizard only allows you to add basic, default information to the card. It does not allow you the flexibility that adding a card manually does.

However, once you have added a card using the Card Wizard, you can go back and add more specific information to that card.

## ***Using the Card Wizard***

The quickest and easiest way to add cards is to use the Card Wizard. With the Card Wizard, you can add one card or a batch of cards.

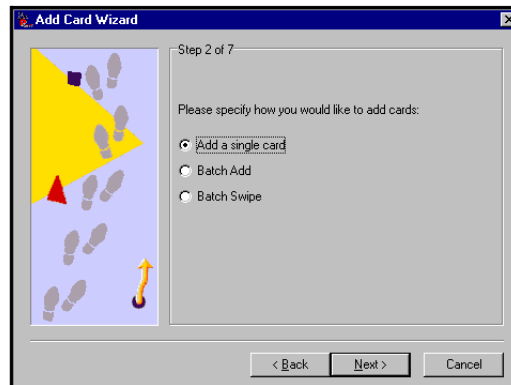
The Card Wizard appears automatically as the last step of the configuration process:



The Card Wizard works in the same manner as the Setup Wizard (shown earlier in this guide). To use the Card Wizard, simply follow the instructions and answer the prompts.



The first step is to determine whether you want to add one card or a batch of cards. Make your selection by choosing the appropriate option:



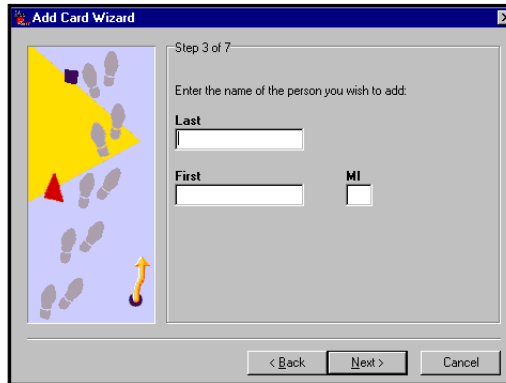
### ***Adding a single card***

To enter a single card using the Card Wizard:

- 1. Select *Add a single card* in the Wizard and click *Next*.**

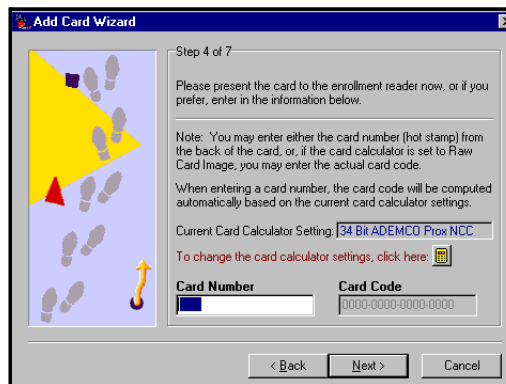
The Wizard will ask you to enter a last and first name for the Cardholder (i.e., the person to whom the card will be

assigned):



- 2. Enter the appropriate name information into the fields and click *Next*.**

The system will prompt you to enter card information:



If you have a Card Enrollment Kit, you can swipe the card at your enrollment reader to enter the card information. Otherwise, key the applicable card information into the screen manually.



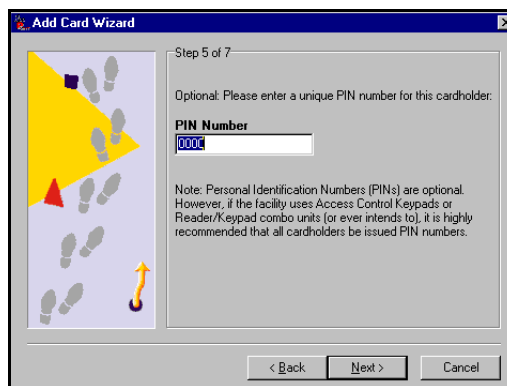
---

The default card setting is 34-bit Ademco proximity.

---

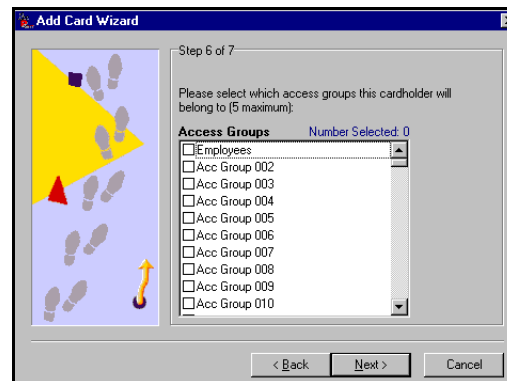
**3. Enter the card information and click *Next*.**

The Wizard will ask you to enter a PIN number for the card. This is an optional step and only needs to be done if your system uses keypad readers that enable a PIN to be used:



**4. Enter a PIN number (if applicable) and click *Next*.**

Next, the Wizard will ask you to choose Access Groups for the card:



Each Cardholder can be assigned to up five Access Groups.

To assign an Access Group to a user, simply check the number of the group(s) in the boxes provided.



---

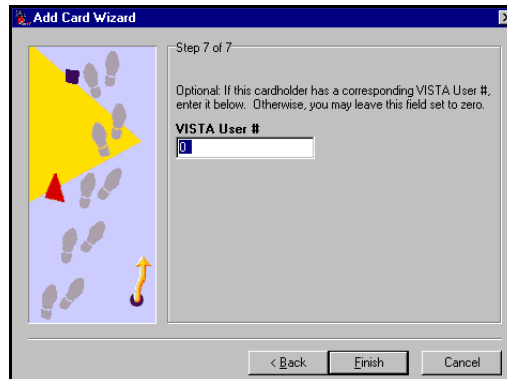
The ASK template includes one pre-set Access Group, called EMPLOYEES. This enables you to choose an Access Group without first having to create one. Later, you can modify or delete the EMPLOYEES Access Group if you want.

---

In order for a Cardholder to have any access privileges at all, he/she must be assigned to at least one Access Group (unless the Cardholder has been granted executive privileges).

**5. Select the Access Groups for the card, then click *Next*.**

The last step is to enter a Vista user number (if applicable):



If the Cardholder has a corresponding Vista user number, enter it in the field provided. If not, leave this field blank.

**6. Click *Finish*.**

The card will be added to the Cardholder database. From here you can view, edit, or delete the card.

## ***Adding a batch of cards***

There are two ways to add a batch of cards: batch add and batch swipe.

### **Batch Add**

Batch adding allows you to quickly add a batch of cards at one time. The Card Wizard will ask you to swipe (or manually enter) the FIRST and LAST card in a batch. The cards must be in numerical order for this method to work. Once this is done, PassPoint will automatically enroll both the first and last card, and every card in between.

Using this method does not allow you to enter Cardholder names for the cards. This must be done separately for each card, along with any other specific card information you want to add.

### **Batch Swipe**

The batch swipe method also allows you to add a batch of cards, but this method requires you to swipe each card one by one at a card enrollment reader.

PassPoint will prompt you to choose which Access Group the Cardholder will belong to, and whether you want to assign a name to each card. Then, you will be prompted to swipe your cards.

## Adding Cards Manually

If you don't want to use the Card Wizard to add a Cardholder to the database, you can simply add the card manually. Adding a card manually allows you greater flexibility when adding cards, since there are many more information fields available to you that allow you to customize the card.

To manually add a card, follow the procedure below:

**1. From the *Config* menu, select *Cards>Add New Card*.**

The Card Data dialog box appears:

*Each tab allows you to add/edit different data for the card.*

*Use the Card Data dialog box to add new cards, edit card data, and delete cards.*

The Card Data dialog box allows you to enter various types of information about each card. Each tab of the box displays a different set of data. When creating a new card record, you fill out these fields as applicable. Some of these

fields, like *Last Name* and *Access Groups*, are mandatory. Others need not be filled, or already contain default data that can be used. The fields that you choose to fill out for each card will depend upon the Cardholder, the needs of the installation, and other factors specific to the premises.

## 2. Fill out the fields of the first tab, *Access*.

The first tab of the Card Data dialog box is the only tab that contains fields that must be filled in for the card to function. Each of these tab fields is explained below:

**Name (Last, First, MI)** - Enter the name of the Cardholder in these three fields. The name does not have to be unique, and the manner in which the name is capitalized is not important.

**Card #** - Enter the card number in this field. The card number entered will automatically compute the correct *Card Code*, provided that the proper *Card Technology* has been chosen.

**Card Technology** - In this field, select the proper card technology type that your system is using.



---

This field must be filled in correctly in order for the card to function. By default, this field will read “34 Bit Ademco Prox NCC,” which is the type of card shipped with the Access Starter Kit.

---

**Card Code** - The card code is the actual code embedded in the card. This is the code that the system reads when the card is presented to a reader. This field cannot be edited. It updates automatically according to the *Card #* entered and the *Card Technology* chosen in the two previous fields.

**PIN Code** - In this field enter the 8-digit personal identification number (PIN) that you want to assign to the Cardholder.

Personal Identification Numbers can be 3 to 8 digits long. A system option sets the PIN code length that is used throughout the system. All PIN codes in the system must be unique to a length of 1 digit less than the system PIN length. In other words, if the system PIN code length is set at 4 digits, the first 3 digits of ALL of the PIN codes in the system MUST be unique. The last PIN digit is a “don't care” — any PIN digit can be assigned in this position. However, never define a PIN code that ends in “0.” This is because any PIN code typed in at an Access Point that ends in “0” may be interpreted as an access request under duress. It might be wise to assign PIN codes that all end in the same digit — for instance, “9.” This is because other special “last” digits may be used by future versions of the system. Note that if a card ID is not entered for this Cardholder (as might be the case of PIN-only systems), data MUST be entered in this field.

**Access Groups** - In the list boxes provided, select up to five Access Groups for the card.

In order for a Cardholder to have any access privileges at all, he/she must be assigned to at least one Access Group (unless the Cardholder has been granted executive privileges, as explained above).

**Disabled** - If you should want to disable the privileges of the Cardholder, check this box. While disabled, all of the Cardholder's access privileges will be revoked. You can reinstate the Cardholder's privileges at any time by unchecking this box. While disabled, the card will remain in the system database. When disabling a card, enter a date



that tells the system when to disable the card.

**Use Expiration Date** - If you want the card to become invalid after a specific date, check this box and enter the date in the field provided. Any attempted use of the card after this date will be denied.

**Use Expiration Count** - If you want the card to become invalid after a specific number of uses, check this box and enter the number of valid uses in the field provided. For example, enter "10" in this field if you want the card to allow only ten access grants.

**Refresh Count** - Refresh the expiration count from the MLB.

**Vista User #** - If there is a Vista control panel user number associated with the Cardholder, enter the applicable number in this field.

**Executive Privileges** - Check this box if you want to grant the Cardholder executive privileges: full access to all of the system Access Points. The Access Groups assigned to the Cardholder will not be checked, so it is not strictly necessary to assign any Access Groups to the reader (although it is highly advisable, since executive privileges are revoked whenever the system is in Threat Level 5).

Note that enabling this field may have security ramifications that must be managed by the system's administrator. Also, if threat levels are used by the facility, any Executive Privilege card should also be assigned at least one Access Group. The Access Group assigned **MUST** be valid during Threat Level 5 so the person will have an escape path from the premises. Not providing such an escape path can have life and safety implications. Executive Privilege cards also retain all the access privileges of all Cardholder Authority

Levels.

**Trace** - Check this box if you want to log a trace event each time the card/PIN code is used. A trace event appears in the event log of the system and “traces” the movements and actions of the Cardholder. Generally, this field will not be used unless a card needs to be “watched” for some reason.

**3. Fill in the fields of the remaining tabs, or click *Save*.**

At any point after filling in the first tab fields, you can save the card record and add the card to the database.

The remaining tabs of the dialog box allow you to enter additional information for the Cardholder. For example, the *Personal* tab allows you to add personal data about the Cardholder, such as his/her address. The *Summary* tab allows you to view summary information about the Cardholder at a glance.

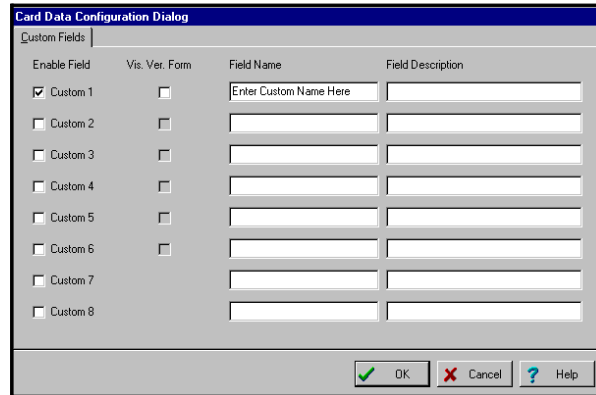
### ***Using the Custom tab***

The *Custom* tab contains user-configurable fields that can include any pertinent information you wish. When you first open the *Custom* tab, it’s essentially blank. This is because no fields have been configured yet.

To configure fields for the *Custom* tab:

**1. From the *Config* menu, select *Cards>Options*.**

The Card Data Configuration dialog box appears:



This dialog box contains various fields that let you customize the *Custom* tab.

**2. Check off the boxes of the fields you want enabled.**

**Enable Field** - This will allow users to type into these fields in the *Custom* tab of the Card Data dialog box.

**Vis. Ver. Form** - Check this box if you want the field displayed on the Visual Verification dialog box.

**Field Name** - In this field, enter the text to be used as the title of the field in the *Custom* tab.

**Field Description** - In this field, enter the text to be used as the help text for the field in the *Custom* tab.

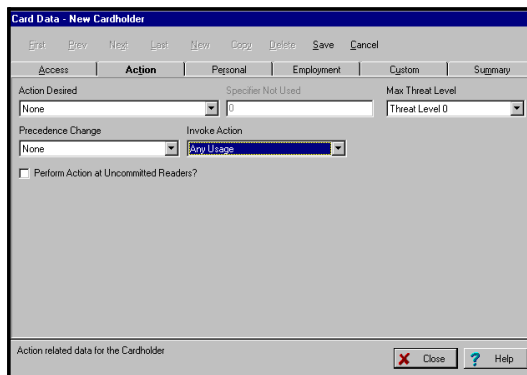
**3. Click *OK*.**

The system will automatically update the information for the *Custom* tab. Next time you open the Card Data dialog box, the *Custom* tab will reflect the data you just entered.

## Using the Action tab

You can configure the system to perform a specific action whenever a specified event occurred with the card (such as an access grant). To do so, use the fields of the Action tab:

*Use the Action tab to associate an action with the use of the card.*



The screenshot shows a dialog box titled "Card Data - New Cardholder" with a menu bar (Edit, Prev, Next, List, New, Copy, Delete, Save, Cancel) and several tabs (Access, Action, Personal, Employment, Custom, Summary). The "Action" tab is active. It contains the following fields:

- Action Desired:** A dropdown menu with "None" selected.
- Specifier Not Used:** A text field containing "0".
- Max Threat Level:** A dropdown menu with "Threat Level 0" selected.
- Precedence Change:** A dropdown menu with "None" selected.
- Invoke Action:** A dropdown menu with "Any Usage" selected.
- Perform Action at Uncommitted Readers?

At the bottom of the dialog, there is a label "Action related data for the Cardholder" and buttons for "Close" and "Help".

**Action Desired** - This is the function you want to occur when the card is used. Make your selection from the predefined list of actions.

**Specifier** - This is the system item acted upon. For instance, if you've chosen "Relay On" as your action, the specifier would be the relay number.

**Maximum Threat Level** - This is the threat level at which the action will be allowed to take place. If the system threat level goes beyond the setting for the action, the action will not be allowed to occur. The default value for this field is 0, meaning normal.

**Precedence Change** - This field indicates how the precedence level of the Specifier (above) will be affected when the action takes place. You can choose None, Clear the precedence level

to 0, or Update to have the resource take on the precedence level of the Cardholder

**Invoke Action** - In this field, select the specific system occurrence upon which you want the action to occur. The action will only take place when the card encounters the situation specified in this field. For instance, you can select the action to occur when an access request is granted. Or you can select the action to occur when an access request is denied.

**Perform Action at Uncommitted Readers** - Check this box if you want the action specified to occur when the card is used at an uncommitted command reader.



Chapter

# 4

## *Setting Administration Options*

This chapter explains how to set several system-wide PassPoint parameters. In this chapter you will learn:

- **How to set access options**
- **How to select preset card format information**
- **How to set Access Point parameters**
- **How to use precedence settings**

## PassPoint Administration Options

Administration options are system-wide parameters that affect how PassPoint operates on a day-to-day basis. Administration options differ from configuration options in that they may be changed more frequently and may be changed by “lower” level system users (i.e., operators and managers).

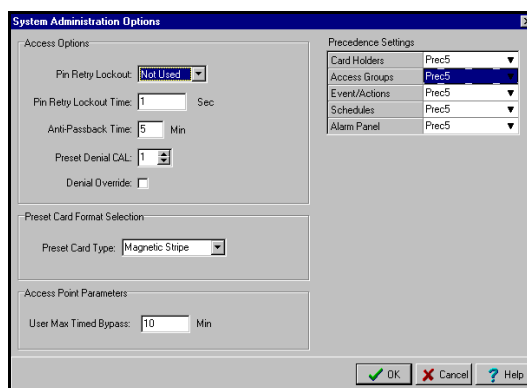
Administration options include:

- **Access options**
- **Preset card format selection**
- **Access point parameters**
- **Precedence settings**

Each of these administration options is explained in detail in this chapter.

All administration options are set in a dedicated dialog box, called System Administration Options. To reach this dialog box, select *Admin* from the *Config* menu:

*Use this screen to set your system administration options.*





### **Setting your administration options**

Use this dialog just as you would any other PassPoint dialog box. Enter the data as necessary in the applicable fields. Some fields require you to choose from system presets. Other fields allow you to enter data directly from your keyboard. A detailed description of each field is provided in the following section.

When you are done setting your administration options, click *OK*.

### **Administration dialog box fields**

Below is a description of each field of the System Administration Options dialog box:

#### **Access options**

The fields in this section control how the system deals with certain access situations.

**Pin Retry Lockout** - How many times do you want an occupant to be able to enter an invalid PIN code before the system locks out the keypad? You can select from 1 to 6 attempts, or you can leave the default choice, “not used,” if you don’t want to use this feature.

**Pin Retry Lockout Time** - How long do you want your keypads to stay locked out after an occupant has continually entered an invalid PIN code (as explained above)? You can enter any number up to 65535 seconds in this field. In low-security applications, the number of seconds that the entry side is locked out should be just enough to discourage people from tampering with the PassPoint system by “trying all possible codes.” In higher security applications, it may be desirable to lock out the entry side of the Access Point for

longer periods of time - possibly long enough to dispatch a guard.

**Anti-Passback Time** - How long do you want the system to wait between access or egress attempts on the same card at the same card reader? This feature, known as anti-passback, prevents a person from gaining access by using a card that was “passed back” to him/her by a Cardholder who has already used the card to enter the same area. Once a card has been used at an Access Point, it cannot be used again to pass in the same direction at that Access Point for the specified amount of time.

You can program any amount of time up to 60 minutes in this field, although you should be careful not to make this time too long, since Cardholders often need to pass through the same Access Point a number of times a day.

**Preset Denial CAL** - The CardHolder Authority Level (CAL) defines what system functions the card can perform.

**Denial Override** - Denial Override is a feature that allows systems requiring more configuration programming to be commissioned gradually. Turning Denial Override on, by checking this box, will automatically grant access to any CardHolder who otherwise would have been denied. The Event History Log will indicate that the access was granted under denial override, and indicate the reason why the card would have been denied.



This feature can be useful in the early stages of commissioning the system. However, it is important that the occupants of the premises know that the system is not protecting them in the normal way. As the system's schedules and Access Groups gradually get programmed correctly, the number of Cardholder access and egress grants that are given under Denial Override will diminish. The system administrator can review the Event History Log for the period this feature was in effect and look for problems with the schedule and Access Group programming of the system.

---

### ***Preset card format selection***

There is only one field in this area, used for entering information about your default ID card type.

**Preset Card Type** - What format of ID cards are you using? You can select among Weigand cards, proximity cards, magnetic stripe cards, and keypads.

### ***Access Point parameters***

**User Max Timed Bypass** - PassPoint operators can initiate a bypass of an Access Point for a predetermined amount of time. This field defines the maximum length of time that the bypass can last. For instance, if the operator chooses to bypass an Access Point for 20 minutes but the number set in this field is 10 minutes, the operator will not be able to initiate the bypass. He/She will only be able to initiate a bypass up to 10 minutes long. The maximum number of minutes for this field can be set at any number between 1 and 65535.

## ***Precedence settings***

All hardware resources (i.e., Access Points, relays, readers, triggers, and zones) have a *precedence level* assigned to them. This precedence level, which can be between 0 (none) and 5 (the highest), defines who or what can control the resource. The who or what can be a Cardholder, an Access Group, an event-action, or an alarm panel. In order for one of these items to be able to control a resource, it must have a precedence level greater than or equal to the precedence level of the resource.

If you want to use the PassPoint precedence feature, select a precedence value for each item in this list provided.

Chapter

5

# *Access Groups*

This chapter explains PassPoint Access Groups, a way of grouping Cardholders who share common system privileges. In this chapter you will learn how to:

- **Create Access Groups**
- **Assign time schedules to Access Groups**
- **Assign Access Points to Access Groups**
- **Enable and disable Access Groups**
- **Setting Entry/Exit control for Access Groups**

## ***What Are Access Groups?***

An Access Group is a collection of Cardholders who share common access privileges. In its simplest sense, an Access Group defines which Access Points may be used by a Cardholder and when they may be used. When you create an Access Group, you define all the parameters that control how it functions. Then, when you assign a Cardholder to the Access Group you've created, the privileges of that Cardholder to use Access Points will be governed by the Access Group.

### ***Access group parameters***

When you create an Access Group, there are three different areas of the Access Group that you must configure in order for it to function properly. All three configuration areas are covered in this chapter. They are:

- **Attributes**

Here you define such things as the Access Group's name and what threat level it is valid under. You can also associate an action with the Access Group, to be performed whenever a Cardholder belonging to the group identifies himself/herself to a valid Access Point.

- **Schedules**

Here you define what time schedules apply to the Access Group. Time schedules will control when the Access Group is valid and when it is not.

- **Access Points**

Here you define what Access Points the Access Group has control over. Only those Access Points specified here can be accessed by the group.

To begin creating Access Groups, start with the first parameter area, attributes. See the next section of this chapter for instructions.



Creating Access Groups does not automatically apply them to Cardholders. After creating an Access Group, you must apply it to your Cardholders individually. Each Cardholder can belong to up to five different Access Groups.

## Creating Access Groups and setting attributes

The creation of an Access Group starts in the Access Groups dialog box. To create an Access Group and set its attributes, follow the procedure below:

### 1. From the *Config* menu, select *Access Groups*.

The Access Groups dialog box appears:

*Use this dialog box to create and edit Access Groups. The tabs contain various information about the Access Group.*

The screenshot shows the 'Access Group 1' dialog box with the 'Attributes' tab selected. The 'Name' field contains 'Acc Group 001'. The 'Authority Level' is set to 'CH1' and 'Threat Level' is 'Threat Level 0'. Under 'Vista Partition Armed Away Restriction', there are eight checkboxes labeled 'Part 1' through 'Part 8', all of which are unchecked. In the 'Action' section, 'Action Desired' is 'Not Used', 'Specifier Not Used' is '0', and 'Max Threat Level' is 'Threat Level 0'. 'Precedence Change' is set to 'None' and 'Invoke Action' is 'Access Grant'. There is a 'Notes' text area at the bottom. The dialog box has a title bar 'Access Group 1' and a menu bar with 'First', 'Prev', 'Next', 'Last', 'Clear', 'Save', and 'Cancel'. A dropdown menu shows '[GRP 001] Acc Group 001'. At the bottom right, there are 'Close' and 'Help' buttons.

When you first call up this screen, the *Attributes* tag is displayed. The elements in this screen define basic parameters about how the Access Group will function.

To create an Access Group, all you have to do is fill in the fields of the tabs, assign a name to the Access Group, then click *Save*. With PassPoint, you can create up to 128 different Access Groups. The list box at the top right of the dialog box lists all of your Access Groups. Since you haven't named or created any groups yet, all of these 128 Access Groups will simply have a number name, e.g., *Acc Group 001*.

**2. In the *Name* field, enter a name for the Access Group.**

You should choose a name that describes the type of people who will belong to the group. For instance, if this Access Group will be applied to regular employees, you can name the group Regular Employees.

**3. Choose a *Maximum Threat Level* for the Access Group.**

The maximum threat level indicates the threat level at which the Access Group will be valid (i.e., be allowed to function). If the system's threat level goes beyond the setting for the Access Group, the Access Group will become invalid. The default value for this field is 0, meaning normal.

**4. In the area labeled *Vista Partition Armed Away Restriction*, select the Vista partitions that must NOT be armed away before access is granted.**

This is an optional step, and can only be set for PassPoint systems connected to an Ademco Vista series control panel.

Select the checkbox for each control panel partition that must NOT be armed away in order for a member of the Access Group to be granted access to it. For instance, if you select the checkbox for partition number 1, a member of this Access Group will not be able to access this partition if the partition is armed away.



**5. In the area labeled *Action*, select an action and the details of what should occur. (Optional)**

Each Access Group can be assigned an action that will take place whenever a Cardholder assigned to the group enters or exits a valid Access Point. There are five fields that need to be completed in order for this optional feature to function:

The *Action Desired* is the function you want to occur when a Cardholder enters or exits an Access Point. Select the action from the predefined list.

The *Specifier* is the system item acted upon. For instance, if you've chosen "Relay On" as your action, the specifier would be the relay number. In this case, you would enter the number of the applicable relay in this field.

The *Maximum Threat Level* indicates the threat level at which the action will be allowed to take place. If the system threat level goes beyond the setting for the action, the action will not be allowed to occur. The default value for this field is 0, meaning normal.

The *Precedence Level Change* indicates how the precedence level of the Specifier will be affected when the action takes place. You can choose "None," "Clear the precedence level to 0," or "Update" to have the specifier take on the precedence level of the Access Group.

Lastly, in the area labeled *Invoke Action Upon*, select when the action should occur. For instance, you can have the action occur whenever a member of the Access Group is granted access, when they are granted egress, etc.

**6. To save the Access Group, click *Save*.**

Clicking *Save* saves the information you've just entered. From here you can go on to create other Access Groups, but

you still need to assign schedules and Access Points to the Access Group you have just created. This is covered in the following section.

## ***Assigning schedules to an Access Group***

Assigning time schedules to an Access Group allows you to control the times that an Access Group is valid. When a time schedule is valid, so are any Access Groups that have that time schedule assigned as a parameter. If a time schedule is not valid, neither is the Access Group.



You must have already created time schedules for your system before you can assign them to Access Groups. Access groups cannot function without valid time schedules to tell them when to operate. Refer to Chapter 6 of this guide for instructions on creating system time schedules.

---

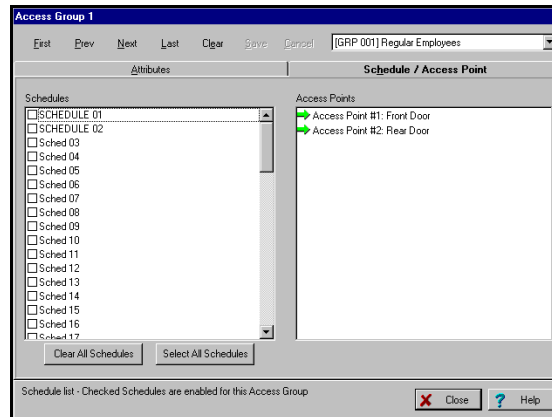
To assign time schedules to Access Groups, follow the procedure below:

- 1. In the Access Groups dialog box, click the *Schedule/Access Point* tab.**

From the *Edit Access Group* menu, select *Define the Schedules During Which an Access Group may Pass*.

This tab displays all of your time schedules and Access

Points:



**2. Select the schedules you want applied to the Access Group.**

To select a schedule, simply click on its checkbox. You can apply all the time schedules to the Access Group by clicking the *Select All Schedules* button.

**3. Click *Save* to save your changes.**

***Removing a schedule from a group***

You can remove a time schedule from an Access Group at any time simply by clicking on its checkbox again. Any checkbox that is not checked is not applied to the Access Group. If you want to remove all the time schedules from the Access Group, click the *Clear All Schedules* button.

## Assigning Access Points to an Access Group

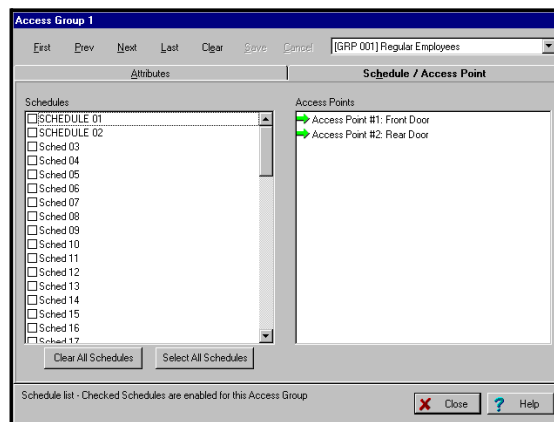
Each Access Group defines one or more Access Points that may be used by the members of the group. Access groups also determine the direction through which the group members may pass through an Access Point (entry, exit, or both).

It is up to you to apply Access Points to each Access Group you create.

To apply Access Points to a group, follow the procedure below:

- 1. If necessary, click on the *Schedule/Access Point* tab in the Access Groups dialog box.**

All of your system's Access Points are listed on the right-hand side of the dialog box:



- 2. Click on the Access Point you want to add to the group, and select how you want it to function.**

By clicking multiple times on an Access Point, you can choose how you want it to function for the applicable Access Group. In the example above, both Access Points

are entry points. That is, this Access Group will be allowed to enter these Access Points. This is denoted by the green entry arrow. Depending how the Access Point is configured, you can choose from the following four options:



Entry



Exit



Both Entry and Exit



Neither Entry nor Exit. In this case, the Access Point will be completely inaccessible to the Access Group.

All four entry/exit options will only be available on Access Points that are both entry and exit. For instance, if your Access Points are all entry points without exit readers, you will not be able to choose the “Exit” or “Both” options. You will only be able to select “Entry” or “Neither.”

### 3. Click *Save*.

Clicking *Save* saves your changes. If you close the Access Groups dialog box now, the system will prompt you to save your changes to the database. If you are happy with the Access Groups you’ve created, you should download them now so that the database will be aware of them.

## ***Disabling and Enabling Access Groups***

There may be times when you will want to temporarily revoke the access privileges of certain Access Groups. These may be emergency situations, times when the building is closed for maintenance, etc.

To disable/enable Access Groups, follow the procedure below:

- 1. In the main PassPoint window, right-click on the Access Group you want to enable/disable.**
- 2. Select *Enable* or *Disable* from the menu.**

The Access Group you selected will be enabled or disabled. A message will appear in the event list explaining which Access Point has been disabled and by whom.



---

Disabling Access Groups can disable an occupant's ability to exit the building (if exit readers are used). Always make sure that occupants have a valid and usable path of egress from the premises.

---

## ***Entry/Exit Control***

Entry/Exit control is a means of controlling and monitoring the flow of Cardholders through a building. It's used in conjunction with Access Groups to either allow or deny group members to specific areas.

### ***How does Entry/Exit Control work?***

The readers on either side of a two-reader Access Point can control access to two different areas in a facility. As Cardholders move through the facility, the area they are moving into is recorded in the Cardholder record. If the card is presented in an unexpected area, the condition is treated as an "Entry/Exit" violation and access can be granted or denied depending on the way the function is programmed. Cardholder events which violate Entry/Exit rules will always indicate that

the exception has occurred and whether or not access was granted.

An *access partition* is a group of related readers at Access Points controlling access to the same area. To create access partitions, Access Point readers are assigned to areas when the Access Point is configured. Each Access Point controls access to two areas if it is assigned to two access partitions. One of the associated access partitions is the area into which the Cardholder enters when she/he traverses through the Access Point via the side\_A reader. The other access partition is the one into which the Cardholder enters when she/he traverses through the Access Point via the Access Point's side\_B reader.

For Entry/Exit to function correctly, the installer must assure that any Access Point which controls traffic between two different areas must be able to identify the each user via a card reader or keypad. If a simple Request To Exit device is used, the system will not be able to recognize the Cardholders and the entry/exit function will fail.

Similarly, if Entry/Exit rules are in effect, it is not safe to schedule Entry/Exit Access Points to bypass or unlock since this would lead to Entry/Exit violations for any Cardholder which uses that Access Point.

***There are three  
Entry/Exit control  
settings***

When configuring Entry/Exit control for your Access Groups, there are three settings you can choose from:

- **None**

Entry/Exit control is an optional ACS feature and does not have to be used. If you select None (the default setting), no Entry/Exit validation will be performed.

- **Soft**

When this setting is applied to an Access Group, validation of the Entry/Exit rules is performed. If an Entry/Exit violation is detected, a Soft Entry/Exit Violation Alert will be logged and, if the Cardholder would otherwise not be granted, she/he is granted access.

- **Hard**

When this setting is applied to an Access Group, validation of the Entry/Exit rules is performed. If an Entry/Exit violation is detected, a Hard Entry/Exit Violation Alert will be logged and the Cardholder is denied access.

When a Cardholder is a member of an Access Group which must abide by Entry/Exit rules attempts to pass through an Access Point, the Cardholder's current area is compared to that of the reader they are using before granting access or egress. If the Cardholder is found to be in the wrong area, an Entry/Exit violation occurs. If the Entry/Exit rule is "hard," the Cardholder is denied access. If the Entry/Exit rule is "soft," the Cardholder is granted access (subject to the other normal rules) and, in either case, the event which is logged indicates that the violation has occurred.

## ***Configuring Entry/Exit control***

1. **In the main PassPoint window, right-click on the applicable Access Group.**

2. **Select *Advanced* from the menu.**

The Advanced options dialog box appears.

3. **In the *Control* section of the dialog box, select the level of Entry/Exit control you want.**



**4. Click Send.**



Chapter

# 6

## *Time Scheduling*

Your PassPoint system has a number of schedule and event related functions for controlling the flow of people through the premises. In this chapter you will learn:

- **How to create Day Templates for each day of the week**
- **How to create time schedules**
- **How to create event-action relationships to link system functions with particular system events**
- **How to re-synchronize schedules**

---

## ***What Is PassPoint Scheduling?***

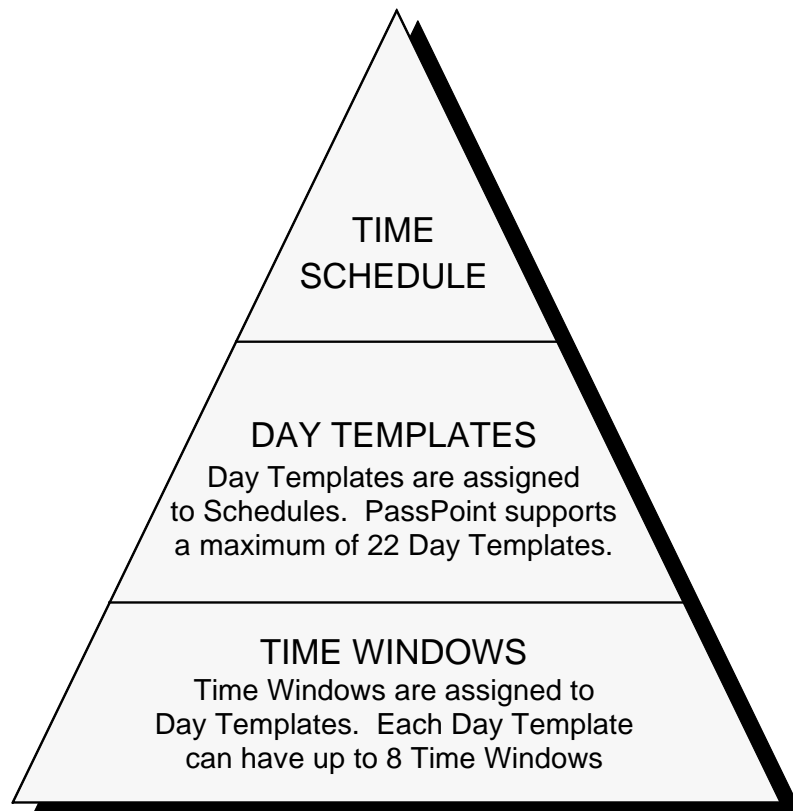
There are a number of functions that your PassPoint system can perform according to certain time parameters. These time parameters are known as schedules. PassPoint has several different types of schedules, but all of them either govern the ability of people to access the premises or cause an event to happen at a particular time.

*For example, Holidays, one feature of PassPoint scheduling, allow you to regulate the access to your premises according to special days when the building might be closed (e.g. Christmas, Independence Day, etc.).*

Essentially, there are two main steps involved in setting up PassPoint schedules. First, you must create Day Templates. Day templates are used to specify the time of day that an action can occur. You can create up to 22 different Day Templates.

Once you've created your Day Templates, you can create your time schedules. You have to create your Day Templates first because Day Templates are applied to schedules. Without Day Templates, a schedule wouldn't know when to function. Day templates dictate when the schedule is "active." You will be reading more about this later in this chapter. For now, you only need to know that you create Day Templates first, and then apply them to time schedules.

To better understand the hierarchy of schedules, refer to the diagram below:



## ***Set the MLB Time***

The Main Logic Board of the PassPoint system must be set to the correct time in order for the system to operate properly. If your system time is not set or is set incorrectly, the system will not unlock doors at the correct times, keep proper track of database events, etc.

To set the MLB time:

- 1. From the *Control* menu, select *Set MLB Time*.**

The system will automatically set the MLB's time according to the time set on the system's PC. In order for the MLB time to be set correctly, the correct time must be set on the system PC.

## ***Day Templates***

The PassPoint system allows you to define *Day Templates*. Day templates are used to specify the time of day that an action can occur. They contain time windows (see below) that define start and stop times for actions. Then, when these Day Templates are applied to *time schedules* (which are discussed later in this chapter), the actions specified in the schedule will occur according to the times defined in the Day Template.

*For example, you can create a Day Template that allows actions to occur only between 10:00 a.m. and 11:00 a.m. You can then apply this Day Template to the “Monday” spot in a time schedule. When that schedule is run, the action specified in that schedule (e.g., unlatching a relay) will only occur between 10:00 a.m. and 11:00 a.m. on Mondays.*

Your system supports up to 22 Day Templates. Two of the Day Templates are predefined. Day template number 1 (01) is preset as “Never.” When applied to a schedule, it means that the action specified in the schedule will never occur on that day. Day template number 2 (02) is preset as “Always.” When applied to a schedule, the action specified will always occur on that day. It is important to note that these two Day Templates cannot be modified. Although they can be viewed on-screen, they are predefined and cannot be changed.

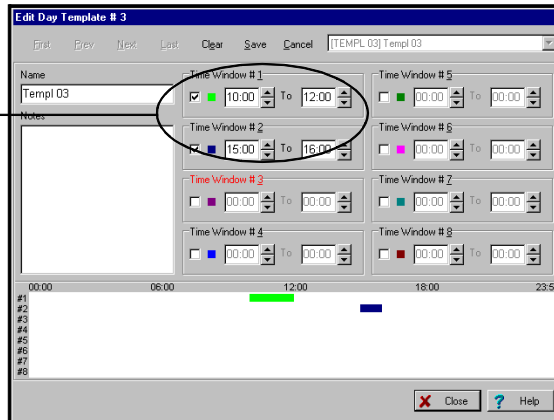
***Each Day  
Template can  
have eight time  
windows***

Aside from the two predefined Day Templates, all other Day Templates can have up to eight *time windows*. Time windows are a way of dividing up the day.

Each time window indicates a period of time during which a schedule that uses the template will be valid. Unlike the “Never” and “Always” templates, the templates you create can vary the times that the action takes place.

For instance, look at the sample Day Template shown below:

*This Day Template uses two of the eight available time windows.*



As you can see, this Day Template (Day Template 03) uses two of the available time windows (1 and 2). If this Day Template is applied to the Monday spot of a schedule, the action specified in the schedule will occur at 10:00 and end at 12:00 on Monday. The action will occur again at 3:00 p.m. and end at 4:00 p.m. All other times during Monday nothing will occur for the schedule, because there are no other time windows specified in the Day Template.

The time that each time window is active is shown graphically at the bottom of the dialog box. Each “bar” appearing in this area represents a different time window. The bars are color-specific for each time window to allow you to quickly view what time windows are active and when they are active.



## ***Creating Day Templates***

When creating Day Templates, there are several things to keep in mind:

- **All time windows must start during the same day.**
- **Time windows cannot overlap.**
- **No time window can begin or end at exactly midnight (24:00).**
- **If a time window ends after midnight, no additional time windows can be added to the Day Template.**

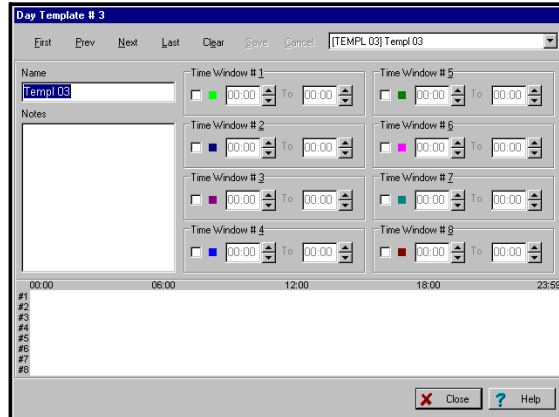
This is true even if there are fewer than the maximum number (eight) of time windows entered for the Day Template.

Although no time windows can start or end at midnight, you can create a time window that spans midnight. For instance, a time window that begins at 23:59 and ends at 23:58 is valid. It will start at 11:59 p.m. on the assigned day and end at 11:58 p.m. the following day.

To create a Day Template, follow the procedure below:

- 1. From the *Config* menu, select *Day Templates*.**

The Day Template dialog box appears:



Here you will name the Day Template you are creating and assign time windows to it. By default, the system will always display Day Template #3 first. Remember, Day Templates 1 and 2 are predefined by the system and cannot be edited.

**2. In the field labeled *Name*, enter a name for the Day Template.**

Type the name for the Day Template directly into the field. You do not choose Day Template names from the name pool.

Choose a name that is representative of the function the Day Template will be performing. For instance, if you are going to be using the Day Template to control a relay for turning on lights, you might name the Day Template “Office Lights.”

If you want to make sure you remember what the Day Template’s function is, enter a description of the Day Template in the *Notes* field.

**3. Enter the start and stop times for the time windows.**

Again, this information is entered directly into the applicable fields. First click in the applicable time window checkbox. Remember to use military format time. As you enter times in the time windows, graph bars will appear at the bottom of the screen representing the times you've chosen for each time window.

**4. Click *Save*.**

Once you have created the template, click *Save* to save the record. The name you have entered for the template will be associated with that template number in the list box at the top of the dialog box.

**5. Click *Next* to create another Day Template, or *Close* to close the dialog box.**

Use the buttons at the top of the screen to navigate through the dialog box. If you want to create/modify the next Day Template, click *Next*. Or, if you want to go to a specific Day Template, choose the applicable Day Template from the list box. Always click *Save* to save your changes for each Day Template. Clicking *Close* closes the dialog box.

## ***Holidays***

In addition to setting up your day templates, you need to set up your system holidays before you start creating time schedules. Holidays are days of the work week when the “normal” work schedule does not apply to your premises.

*For example, Thanksgiving might be a holiday for your premises. Even though Thanksgiving is always on a Thursday, you would not want the normal work schedule to apply to that day of the year if your business is closed. In other words, you don't want to allow people access to the premises on Thanksgiving.*

***Each holiday is assigned a calendar date and day template***

PassPoint allows you to assign 32 holidays. Each holiday is assigned a calendar date and a day template. The calendar date is the actual day that the holiday occurs (December 25 for Christmas, for instance). The day template defines the time windows under which the system will function.

When a holiday is reached, say December 25, the day template you have assigned to the holiday will be substituted for the day template indicated in the system's schedules.

*For example, let's assume you have assigned December 25 as a holiday. Let's also assume you have assigned this holiday day template number 5. If December 25 falls on a Wednesday, day template number 5 will be used on that day, instead of the day template normally assigned to Wednesday.*

There is an exception to the rule above, in that you can also choose day templates for holidays within schedules. If you do this, the day template you choose for the schedule will override the day template chosen for the holiday for that schedule.

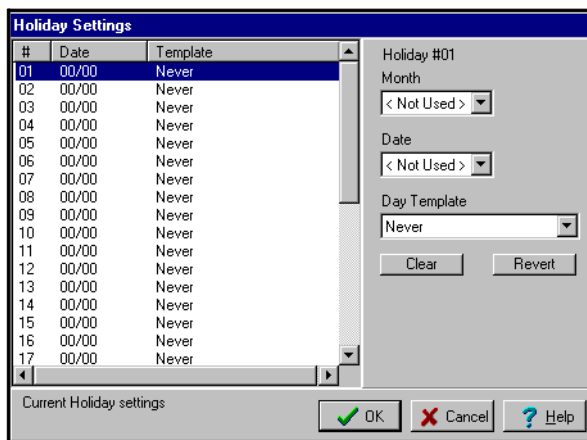
---

## Assigning holidays

To assign your system holidays, follow the procedure below:

**1. From the *Config* Menu, select *Holidays*.**

The Holidays dialog box appears:



Here you assign the dates and day templates for your holidays. You can assign up to 32 holidays.

By default, the system assigns day template 1 to each holiday. Remember, day template 1 is the “Never” template. When this day template is applied to a schedule, the action specified in the schedule will never occur on that day. In the case of a holiday, this might mean that the Access Points never unlock, which might be what you want in the case of a holiday.

**2. Enter the *Month* and *Date* for the applicable holiday.**

Enter the month followed by the day of the month. For instance, for Independence Day, you would choose “July” in the *Month* field, and “04” in the *Date* field.

**3. Enter the *Day Template* for the holiday.**

If you want to use a day template other than the default selection, select the applicable day template number in the field provided.

**4. Repeat steps 2 and 3 for each holiday.**

Again, you can enter as many as 32 holidays.

**5. Click *OK* when done.**

***The Clear and Revert buttons***

In addition to the data fields, the dialog box also contains two buttons, *Clear* and *Revert*. Clicking *Clear* clears the schedule you are editing, returning it to its default state (the Never template). Clicking *Revert* clears the most recent changes in the data fields, reverting them back to the previous data for the holiday.

## ***Time Schedules***

Once you have created Day Templates, you can start creating time schedules.

PassPoint performs actions according to weekly schedules. The system supports up to 64 weekly schedules, all of which you can configure to perform certain actions at certain times. By applying the Day Templates you've created to schedules, you can manage the days and times that Access Points are locked, triggers are energized, burglary zones are bypassed, etc.

*For example, if you wanted PassPoint to automatically energize an uncommitted relay to turn on parking lot lights at 6:00 PM every day of the week, then turn the lights off again at 5:00 AM the next morning, you could create a schedule to do this. The schedule would tell the system what action to perform (energizing and de-energizing the relay). The Day Template applied to each day of the schedule would dictate the times the relay was energized and de-energized. (Keep in mind that the relay's ratings are 5A @ 28V max.)*

**When are schedules active?**

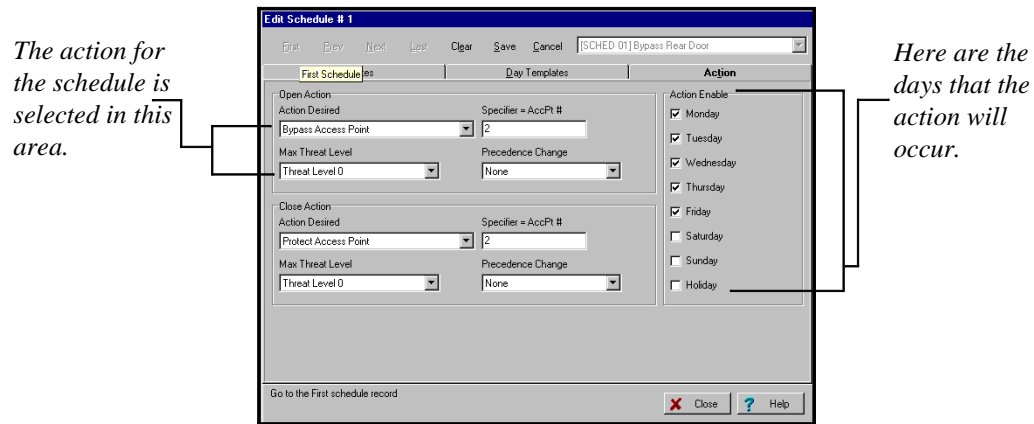
Any schedule can be valid at any given time, provided that the times dictated by the schedule's Day Templates have activated the schedule. In other words, whenever the times in a schedule's Day Templates are reached, the schedule becomes active. Conceivably (although highly unlikely), all 64 schedules can be active at the same time. When a Day Template contains a time window which passes through midnight, that window must finish before any time window can begin on the next day.

*For example, a Day Template for Monday may contain a time window that spans from 11:30PM to 2:00AM. If the Day Template assigned to Tuesday contains a time window that begins before Monday's template ends (for instance, a window may begin at 1:30AM on Tuesday's Day Template), it is ignored until Monday's time window finishes. So, if Tuesday's Day Template contained a time window that spans from 1:30AM to 6:00AM, Tuesday's Day Template will not come into effect until 2:01AM on Tuesday morning.*

**Schedules control actions**

Each schedule is used to control two specific actions. Those actions will function according to the Day Templates assigned to the schedule. You choose the actions that are performed by the schedule from a list of available system functions.

For instance, look at the sample schedule shown below:



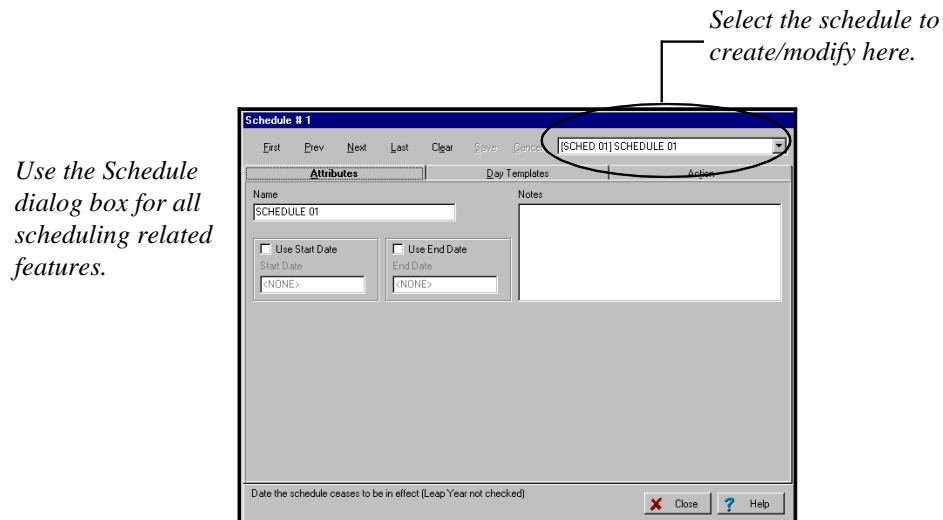
This schedule, named “Bypass Rear Door,” could be used to unlock the rear door of a building at the specific times denoted by the Day Template assigned to it. The Day Template, which appears in a separate tab, tells the schedule when to unlock the door.

The action for the schedule is selected on the left side of the dialog box. In this case the action reads “Bypass Access Point.” The Access Point number to be bypassed is also specified. There are also fields that tell the system what to do when the end of the time window has been reached. In this case, the system will protect the Access Point at the end of the time windows.



## Creating Schedules

All PassPoint scheduling features are set in the Schedule dialog box, shown in the example above and again below:



To reach this menu, select *Schedules* from the *Config* menu.

At the top of the dialog box is a list box listing all of your system schedules. PassPoint can use up to 64 different schedules. As you change schedules in the list box, the *Name* field changes to display the name of the schedule you are creating/modifying.

The dialog box contains three tabs, each of which allows you to set different parameters for the schedule. These tabs are:

- **Attributes**
- **Day Templates**

- **Action**

You have to set information in each of these tabs when creating a time schedule. Start with the first tab, *Attributes*.

### ***Setting Schedule attributes***

The *Attributes* tab lists the name of the schedule, which you can change, the start and end date for the schedule, plus any pertinent notes you want to enter that describe the schedule.

To set the Schedule's attributes:

- 1. In the field labeled *Name*, enter a name for the schedule you are creating.**

Choose a name that describes the action you want the schedule to perform.

- 2. Enter a *Start* and *End* date in the fields provided.**

These dates define how long the schedule will be used. Some schedules you will want to use constantly. Others may be used to perform tasks that you only need done for a short time.

- 3. Enter any applicable notes in the *Notes* field.**

Use this field to enter a description of the time schedule or any other information you think will be helpful.

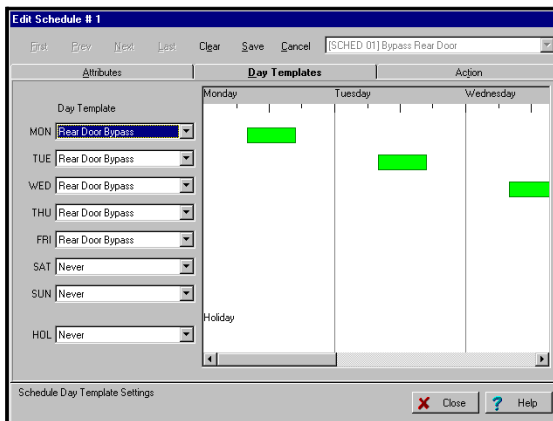
- 4. Click the *Day Templates* tab.**

Once you have set all the attributes for the schedule, you can now assign it Day Templates.

## Assigning Day Templates

The *Day Templates* tab allows you to choose the Day Templates for the schedule:

Select the applicable Day Template for each day of the week.



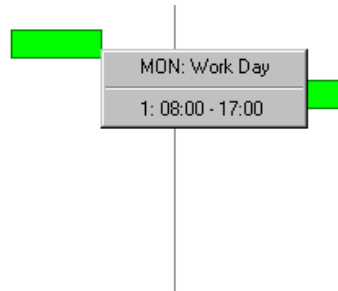
To assign Day Templates to the schedule, simply select the applicable Day Template for each day of the week using the list boxes provided. In the example above, the same Day Template has been used for Monday through Friday. The bars on the right side of the screen indicate when the Day Templates are active for the schedule.

You can only enter one Day Template for each day. However, you can enter multiple Day Templates for each schedule. That is, Monday can be assigned Day Template 3; Tuesday, Day Template 6; etc.

By default, each day of the schedule is assigned Day Template 1, the “Never” template.

**Right-click menu**

Right-clicking in the Day Template field brings up a sub-menu:



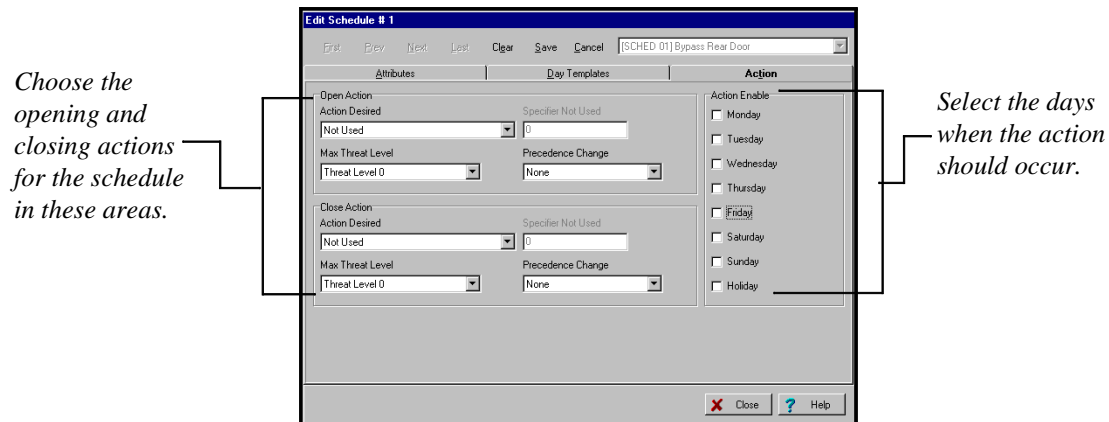
This sub-menu has two parts. The first allows you to quickly go to and edit the Day Template assigned to the day you are currently in. For instance, in the example above, the right mouse button was clicked when the mouse pointer was in the Monday field. Here you can see that the Day Template for Monday is “Workday.” If you want to now edit the Workday Day Template, you can select it from the menu.

The bottom half of the menu simply shows the hours of the day that the Day Template is assigned to Monday.

### ***Assigning actions to Schedules***

Actions are the events that occur when the time schedule is active. Remember that a schedule is active whenever one or more of its Day Templates is active. Therefore, when the schedule is active, the action specified occurs. When the schedule becomes inactive, the action ceases (or more specifically, the “closing action” occurs).

Actions are set in the *Actions* tab:



To assign actions to a schedule, follow the procedure below:

- 1. In the section labeled *Open Action*, choose an action, a specifier, the maximum threat level, and a precedence level change.**

The *Action* is the function you want to occur when the start time for the window is reached. Make your selection from the predefined list. The action may be to turn on a relay, bypass an Access Point, etc.

The *Specifier* is the system item acted upon. For instance, if you've chosen "Relay On" as your action, the specifier would be the relay number. If you've chosen "Bypass Access Point," the Access Point number would be the specifier.

The *Maximum Threat Level* indicates the threat level at which the action will be allowed to take place. If the threat level goes beyond the setting for the schedule, the action will not be allowed to occur. The default value for this field is 0, meaning normal.

The *Precedence Level Change* indicates how the precedence level of the Specifier will be affected when the action takes place. You can choose “None,” “Clear the precedence level to 0,” or “Update” to have the Specifier take on the precedence level of the schedule.

- 2. In the section labeled *Close Action*, enter an action, a specifier, the maximum threat level, and a precedence level change.**

This is the function you want the schedule to perform when the end time of the time window is reached. Typically, this would be the reverse of the first action. For instance, turning off the relay you previously turned on. You can, however, choose a completely different action, such as turning on or off a trigger. The action you select here will depend on your system layout and needs.

- 3. Choose the days of the week for the action(s) to occur.**

Select the days with the checkboxes provided. The actions will only occur on these specified days.

- 4. Click *Save*.**

The schedule you have created will be saved and will begin functioning as soon as appointed action times are reached.

## ***Resynchronizing Schedules***

At times, when system schedules have been accessed a great deal and modifications have been made, it is possible that you may lose track of what schedules are currently valid and invalid, and which have executed their opening actions. When this is the case, you might want to “resynchronize” your system schedules.

Resynchronizing does three things:

- **It brings all precedence levels for your system schedules down to 0**
- **It recalculates your time schedules so that only those that should be valid are valid at the time the resynchronization is performed.**
- **For any valid time schedules, the opening action is performed.**

The opening action is the action you specified for the schedule to perform whenever the schedule first becomes valid.

To resynchronize your system's time schedules, follow the procedure below:

**1. From the *Status* menu, select *Re-Sync Schedules*.**

The system will automatically resynchronize all of the time schedules and execute the opening actions for each one. The event list at the bottom of the screen will indicate that the system precedences have been cleared and that the schedules have been synchronized.





Chapter

7

## *Event-Action Relationships*

Event-action relationships allow system functions to be linked with a system event. Upon the occurrence of the system event, the action is performed.

In this chapter you will learn how to:

- **Use event-action relationships to control your system**
- **Create event-action relationships**

---

## What Are Event-Action Relationships?

Event-action relationships allow system functions to be linked with a system event. Upon the occurrence of the system event, the action is performed.

You can create 32 separate event-action relationships for your system. For each one, you must specify a system event (with a specifier) and a system function (with a specifier). The event defines the trigger for the action. The action defines what actually occurs when the event takes place. Specifiers are used to further define the actions and events.

*For example, you can create an event-action relationship to lock an Access Point (action) upon the arming of a partition (event). In this case the specifiers would be the number of the Access Point to lock and the number of the partition being armed.*

For each event-action relationship, the user can specify time schedule qualifying information. This means that you can have the event-action relationship occur only if a certain time schedule is valid (i.e., currently being used), or only if the time schedule is not valid.



---

Before attempting to create event-action relationships for your system, you should have already created system time schedules. Otherwise you will not be able to specify which time schedules are valid for your event-action relationships.

---

## Creating event-action relationships

To create event-action relationships for your system, follow the procedure below:

1. From the *Config* menu, select *Event/Actions*.

The Event-Action dialog box appears:

It is here that you create and view your system's event-action relationships. You can create 32 in all, but when you first bring up this screen it will be blank, as shown above, and will start with event-action relationship #1.

2. In the section labeled *Trigger*, select an event and specifier in the fields provided.

The *Trigger Action* is the system event that must occur for the action (which you will be entering next) to take place. Make your selection from the predefined list. The event may be the arming of a partition, the faulting of a zone, etc.

The *Specifier* is the system item upon which the event (above) occurred. For instance, if you've chosen "Upon Arming" as your event, the specifier would be the partition number being armed.

- 3. In the section labeled *Action to be Performed*, enter an action, specifier, maximum threat level, and precedence level change.**

The *Action Desired* is the action you want to take place upon the specified event. Make your selection from the pre-defined list. The action may be to execute a script, turn on a relay, etc.

The *Specifier* is the system item to be acted upon. If the action is to turn on a relay, the specifier would be the relay number.

The *Maximum Threat Level* indicates the threat level at which the action will be allowed to take place. If the threat level goes beyond the setting for the schedule, the action will not be allowed to occur. The default value for this field is 0, meaning normal.

- 4. In the section labeled *Schedule Qualification*, enter schedule information for the event-action relationship. (Optional)**

For each relationship you create, you can associate a time schedule with it. In the fields provided, select the applicable time schedule and whether it is valid or not. The event-action relationship will occur according to the information you enter.

For instance, if you select time schedule 002 and “Valid,” the event-action will only occur when schedule 002 is being used. If you select “Not Valid,” the event-action will only occur when schedule 002 is not being used.

- 5. Click *Save* to save the event-action relationship.**
- 6. To create another event-action relationship, click *Next*.**

*Next* brings you to the next event-action relationship.

Repeat the steps above to create as many event-action relationships as you want. To return to a previous event-action relationship, click *Previous*.

**7. Click *Save* when done.**



Chapter

8

# *Precedence Levels*

Precedence levels define when a system resource can be controlled, either by a user or another system component such as a time schedule.

In this chapter you will learn:

- **How PassPoint precedence levels function**
- **How system resources are affected by precedence levels**
- **How precedence levels work with event-action relationships and time schedules**

---

## What is Precedence?

Simply put, precedence levels determine whether or not a manual operation should take “precedence” over any other previously initiated action.

*For example, if an operator permanently bypasses a door in the evening so that the cleaning staff can enter, should the PassPoint schedules resume control over that door at the next schedule change or not? Should an event-action involving this door be blocked or not?*

These are very different questions than those addressed by user levels. User levels determine whether or not members of those levels (such as Operators) ever have the right to exercise specific types of control.

### ***Precedence depends on previous events***

Precedence works differently. Precedence depends on the control events preceding the current one. In the example above, the questions can only be answered if you know the precedence level of the operator who bypassed the door. If the next schedule has a precedence level greater than or equal to the operator’s, the schedule will take precedence and control the door. The same is true of the event-action relationship. Otherwise, if the schedule and event-action relationship have precedence levels lower than the operator’s, neither will be able to control the door.

### ***What resources are affected by precedence levels?***

There are five different system resources that are affected by precedence levels. They are:

- **Access points**
- **Uncommitted readers**



- **Relays**
- **Triggers**
- **Zone inputs**

Each individual system resource starts out with a precedence level of 0. This means that any user can “touch” the resource. Touching a resource simply means being able to control it. If a user cannot touch a resource, it means that he/she does not have the authority to control the resource. Once a resource is touched, it takes on the precedence level of the user that controlled it.

*For example, if an Access Point is touched by an operator with a precedence level of 3, the Access Point will then have a precedence level of 3. At this point, only users with a precedence level of 3 or greater will be able to control the Access Point.*

**Resources are controlled by “Initiators”**

The user who affects the precedence level of a resource is known as an *Initiator*. An Initiator can be more than just a user, however. An Initiator can also be a schedule, a CardHolder, an Access Group, or an event-action. Each of these initiators is given its own precedence level. Whenever the Initiator touches a resource, that resource takes on the precedence level of the Initiator.

*For example, let’s assume you have set your time schedules to have a precedence level of 4. If any time schedule bypasses the back door of your premises, that Access Point will be given a precedence level of 4. Therefore, only an operator with a precedence level of 4 or greater will be able to return the back door to Protect mode.*

In order to keep track of the preceding control events, the MLB contains a table of control precedences. It allows you to set the precedence level for all of the Precedence Initiators.

By default, the precedence levels for PassPoint users and components look like this:

<b>Initiator Class</b>	<b>Precedence</b>
CardHolders	5
Access Groups	5
Event-Actions	5
Schedules	5
Alarm Panel	5

Unless you changed these default settings, all of your Initiators will have a precedence level of 5. 5 is the highest precedence setting, and it means that any Initiator can touch any resource. Even if a resource has been touched and has taken on a precedence level of 5, any Initiator can control it, since all will have a precedence level equal to or greater than that of the resource (5, in this case).



---

If you do not plan on using the PassPoint precedence feature, you can simply retain the default value of 5 for all of your Initiators. This way, all Initiators will be able to control all resources, regardless of the resources' precedence level. Eventually, after all resources have been touched, all resources will have a precedence level of 5.

---

## **Using precedence**

Some resources (most notably Access Points) are involved in a wide variety of control actions. The precedence strategies apply to all of the control actions which can be performed at a single resource, but only one precedence value applies to each resource.

*For example: A reader is scheduled to revert to Protect mode after-hours, but an operator takes control at a higher level of precedence by bypassing the Access Point before the schedule comes into effect. The schedule is prevented from changing the mode.*

### **Resetting resource precedence levels**

The initial precedence value for each controllable resource is 0. If an Initiator has a precedence level high enough to perform a function on a resource, the resource then takes on the precedence value of the Initiator.

However, you can reset the normal precedence level of a resource after it has been touched by an Initiator.

The two precedence level reset commands are:

- **Clear Precedence**

This command simply returns the precedence level of the resource to 0. It does not analyze the system's schedules to determine what the current state of the resource should be.

- **Resume as scheduled**

This command returns the precedence level of the resource to 0, then analyzes all the system schedules that directly

affect the resource. After the schedules are analyzed, the system will determine what state the resource should be in. For instance, the schedules may indicate that an Access Point should currently be bypassed.

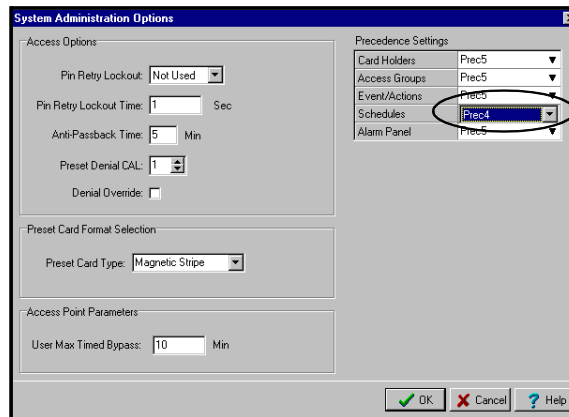
At power-up and after system resets, the system performs the equivalent of a “Resume scheduled control” command on all system resources.

### ***Precedence level scenarios***

Listed below are several use-case scenarios describing how the precedence feature functions under different circumstances. Before reading these scenarios, you should be familiar with most of the other features of PassPoint, including time schedules and event-action relationships.

#### ***Use-Case Scenario 1 - Normal Scheduling***

Let’s assume you have set a precedence level of 4 for all of your system’s time schedules. This would be done in the Edit System Administration Options screen, described in Chapter 4 and shown below:



*Schedules for this PassPoint system have been given a precedence level of 4.*

If an Access Point is under scheduled control from 7:30 until 17:30, the precedence for scheduled control (4, in this case) is assigned to the Access Point when the schedule is first activated. The resource remains at precedence level 4 until it is touched by an Initiator of higher precedence or until it has been manually returned to 0 using the *Clear Precedence* command.

### ***Use-Case Scenario 2 - Illegal manual control***

An operator with precedence level 3 (or less) tries to take control of a scheduled resource in error. Assuming your system time schedules still have a precedence level of 4 (as in the example above), his attempt to control the resource will fail, because he does not have a high enough precedence level. In order to control the resource, he would need a precedence level of 4 or higher (to match that of the schedule).

### ***Use-Case Scenario 3 - Manual control overrides a schedule***

- 1) An operator with precedence 5 overrides the schedule (at precedence 4). The resource remains at precedence 5 and the schedule ceases to be able to control the resource.
- 2) If the operator has a precedence of 4, he will be able to override the schedule but will not be able to take control of it. The schedule will resume control of the resource at the next schedule window.

### ***Use-Case Scenario 4 - Event-action overrides a schedule***

- 1) An event-action with precedence 5 overrides a schedule at precedence 4. The precedence level of the resource is raised to 5, and the schedule loses control over the resource.

2) An event-action with precedence 5 overrides a schedule at precedence 4. The precedence of the resource is then cleared using the *Clear Precedence* command, returning the precedence of the resource to 0. The first Initiator to touch the resource can take control again. An operator with precedence 1 who was previously unable to control the resource can now take control. Once the operator touches the resource, the resource will take on the operator's precedence (1, in this case).

***Use-Case Scenario 5 - Event-action overrides a schedule***

An operator with precedence 5 chooses, for security reasons, to lock an Access Point against all accesses, all scheduling, and all attempts by lower level operators to return the Access Point to normal operation. Now only another operator with precedence 5 can return the Access Point to normal operation, assuming that all other Initiators have a precedence level lower than 5.

Chapter

# 9

## *The Event Log*

This chapter explains the basic use of the PassPoint Event Log.

In this chapter you will learn how to:

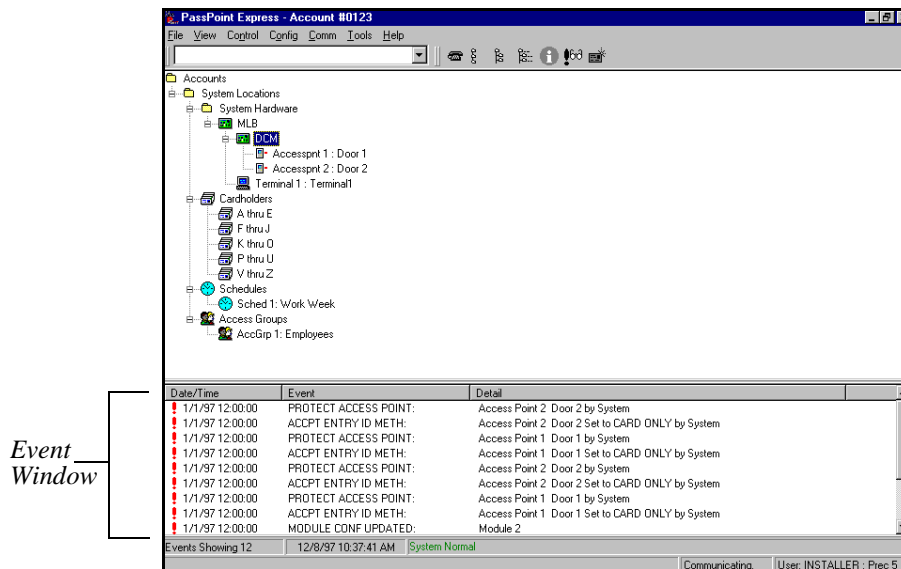
- **View events with the Event Browser**
- **Archive events for future reference**

## What Is the Event Log?

Every time the system detects an action, whether it be a card swiping, an access point opening, etc., it considers the action an event.

In order to help you keep track of all these different actions, the system stores them in a list called the Event Log. The Event Log allows you to keep a record of all system events for reference, trouble-shooting, tracking of Cardholders, or any other purpose where a list of system events is needed.

Events scroll up from the bottom of the screen as they occur, in the part of PassPoint Express known as the Event Window:



The events shown in the Event Window are only for viewing purposes, however. In order to print or store these events,



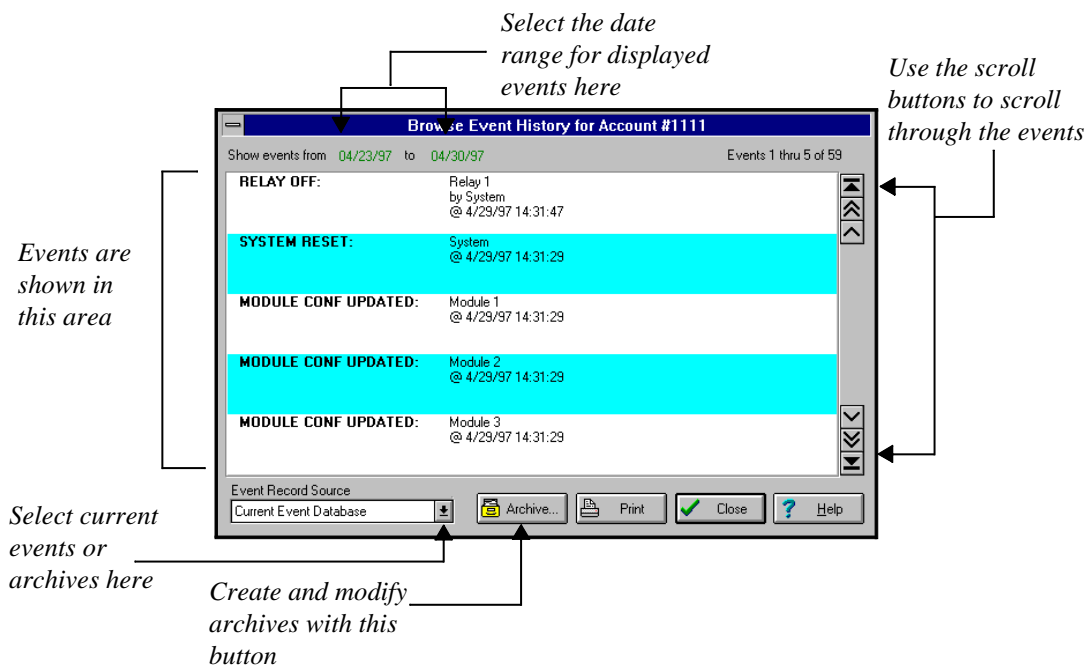
PassPoint uses a tool called the Event Browser. Using the Event Browser, you can view all the current events in the Event Log, print them, or archive them for future reference.

## The Event Browser

The Event Browser organizes all of the events by date and displays them on an easy-to-navigate screen. You can call up the Event Browser at any time and view the events stored on your PC.

### Using the Event Browser

To start the Event Browser, click the Event Browser button, or select *Event Browser* from the *View* menu. The Event Browser will appear, listing any events that are currently on-screen:



The Event Browser displays five events at a time. You can scroll through the events using the different scroll buttons on the right of the screen. These buttons let you scroll one event at a time, scroll five events at once, or scroll immediately to the top or bottom of the event list.

**Changing the date range**

At the top of the Event Browser screen are two dates. This is the range for which events are shown in the screen. You can change this range to either expand or narrow the number of events shown in the Browser simply by clicking on one of the dates. Clicking on the dates calls up a calendar in which you can change the start or end date range (depending on which date you click).

**Archiving events**

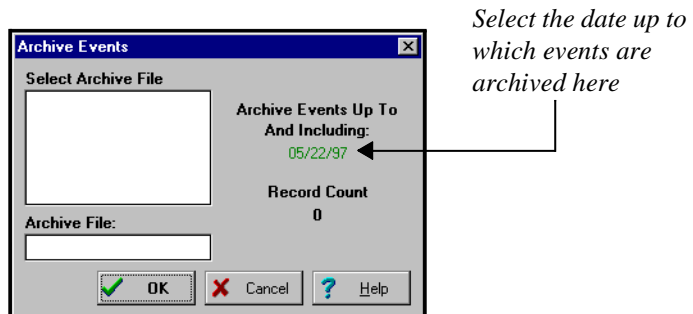
When you first bring up the Event Browser, it will display the current event database. This is the Event Log you have just uploaded. However, once you start uploading events on a regular basis, you will need to archive events. Archives are files that hold past events. You can create archives as you need them, and can name them according to whatever naming scheme works best for you. Generally, archives are meant to be named according to the dates of the events stored within them.

*For example, if you have archived a group of events for the month of April, you might name the archive "April."*

To create an archive:

**1. Click the *Archive* button.**

The Archive Events dialog box appears:



**2. Using the *date* field, select the date up to which you want to archive events.**

Clicking the *date* field brings up a calendar from which you can select a date. All the uploaded events will be archived up to and including the date you specify here.

**3. Enter a name for the archive.**

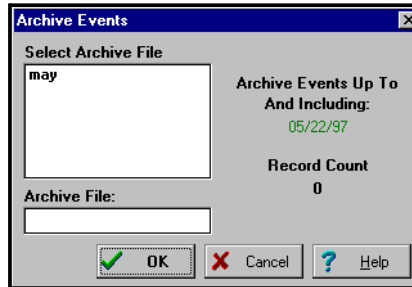
In the *name* field, enter a descriptive name for the archive. Again, a date range might be a good naming scheme to use. The name can be up to eight characters in length.

You can also choose an existing archive. If you do so, the new events will be added to the existing archive. The old data will not be erased, it will simply be appended.

**4. Click *OK*.**

Your archive will be created. It will appear in the Archive Events dialog box the next time the *Archive* button is clicked.

*Once you create an archive, it appears in the dialog box.*



### ***Viewing an archive***

Once you have created an archive, you can view the events within it using the Event Browser. By default, the Event Browser displays the events in the current Event Log. You can change the Browser's view by clicking the drop-down list box at the bottom left of the Browser screen. Any archives you have created will appear in this list. Once you select an archive, the Event Browser will change to display the archive's events.

Chapter

# 10

## *Setting System-Wide Options*

This chapter explains how to set several system-wide PassPoint parameters. In this chapter you will learn how to:

- **Set system presets**
- **Set card technologies**
- **Set up and use Skeleton codes**
- **Set burglary system options**
- **Set dialer reporting options**
- **Set modem parameters**
- **Set network/ID parameters**
- **Set system priorities**

---

## ***PassPoint System-Wide Options***

System-wide options are parameters that control certain aspects of the system's operation. By setting these options to the needs of your installation, you can tailor the system to the needs of your premises.

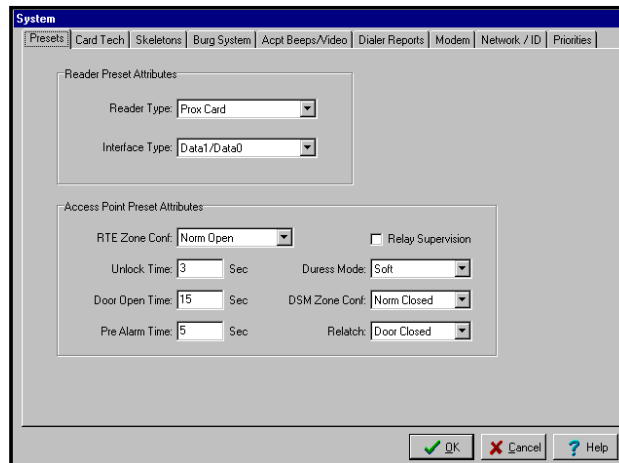
System-wide options include:

- **Presets**
- **Card technology**
- **Skeleton codes**
- **Burglary system options**
- **Access point beeps/video**
- **Dialer reporting options**
- **Modem parameters**
- **Network/ID parameters**
- **System priorities**

Each of these options is explained in detail in this chapter.

All system-wide options are set in a dedicated dialog box, called System. To reach this dialog box, select *System Wide Options* from the Installer Configuration dialog box:

*Use this screen to set your system wide options.*



### **Setting your system-wide options**

Use this dialog just as you would any other PassPoint dialog box. Enter the data as necessary in the applicable fields. Some fields require you to choose from system presets. Other fields allow you to enter data directly from your keyboard. A detailed description of each field is provided in the following section.

When you are done setting your options, click *OK*.

## System presets (*Presets tab*)

This screen allows the installer to choose some hardware configuration parameters that will be invoked when adding hardware items to the system. Setting these fields to values that will be used most often will save you time when configuring new hardware, since these settings will automatically be invoked for you when you add hardware to the system.

The screenshot shows a software window titled "System" with a menu bar containing "Presets", "Card Tech", "Skeletons", "Burg System", "Acpt Beeps/Video", "Dialer Reports", "Modem", "Network / ID", and "Priorities". The window is divided into two main sections: "Reader Preset Attributes" and "Access Point Preset Attributes".

**Reader Preset Attributes:**

- Reader Type: Prox Card (dropdown menu)
- Interface Type: Data1/Data0 (dropdown menu)

**Access Point Preset Attributes:**

- RTE Zone Conf: Norm Open (dropdown menu)
- Relay Supervision:  (checkbox)
- Unlock Time: 3 (text input) Sec
- Duess Mode: Soft (dropdown menu)
- Door Open Time: 15 (text input) Sec
- DSM Zone Conf: Norm Closed (dropdown menu)
- Pre Alarm Time: 5 (text input) Sec
- Relatch: Door Closed (dropdown menu)

At the bottom of the window are three buttons: "OK" (with a green checkmark), "Cancel" (with a red X), and "Help" (with a question mark).



Changing options here does not change settings in pre-existing configured options. These presets will be used the time you add equipment to your system. You can then reconfigure the equipment if you want to customize a component further.

### ***Reader preset attributes***

**Reader Type** - In this field, select the type of card reader, keypad, or a combination unit that you will be using throughout the installation. Note that although this setting will be



automatically filled in for you when you assign readers to the system, you can override them by selecting another reader type when you configure the individual hardware modules.

**Interface Type** - In this field, select the electrical interface that will be used by your readers. Note that although this setting will be automatically filled in for you when you assign readers to the system, you can override it by selecting another interface type when you configure the individual hardware modules.

### ***Access Point preset attributes***

**RTE Zone Conf** - Select the zone configuration that will be used for RTE zones. Note that although this setting will be automatically filled in for you when you assign RTE zones to access points, you can override the setting by selecting another zone configuration type when you configure the individual access points.

**DSM Zone Conf** - Select the zone configuration that will be used for DSM zones. Note that although this setting will be automatically filled in for you when you assign DSM zones to access points, you can override the setting by selecting another zone configuration type when you configure the individual access points.

**Unlock Time** - Enter the default unlock time for access points. Note that although this setting will be automatically filled in for you when you configure access points, you can override the setting by changing the unlock time when you configure the individual access points.

**Door Open Time** - Enter the default door open time for access points. Note that although this setting will be automatically filled in for you when you configure access points, you can

override the setting by changing the door open time when you configure the individual access points.

**Pre-Alarm Time** - Enter the default pre-alarm time for access points. Note that although this setting will be automatically filled in for you when you configure access points, you can override the setting by changing the pre-alarm time when you configure the individual access points.

**Relay Supervision** - Check this box if you want the relay supervision feature for access points enabled when you configure a new access point. Note that although this setting will be automatically filled in for you when you configure access points, you can override the setting by changing the relay supervision option when you configure the individual access points.

**Relatch** - In this field, choose the relatch option for access point door control relays. Note that although this setting will be automatically filled in for you when you configure access points, you can override the setting by changing the relatch option when you configure the individual access points.

In general, when using electromagnetic locks, use relatch on close. When using door strikes, use relatch on open.

**Duress** - In this field, choose the duress mode setting for access points. Note that although this setting will be automatically filled in for you when you configure access points, you can override the setting by changing the duress setting when you configure the individual access points.

## Card technology options (Card Tech tab)

In order for PassPoint to communicate properly with your door control hardware (i.e., card readers), it must be informed of certain parameters.

For example, the system must know how many bits of information the cards you are using contain. The system also needs to be given “recognizer” information so that it can decipher the data on ID cards and try to recognize them.

The screenshot shows the 'System' configuration window with the 'Card Tech' tab selected. The window contains a table of 'Card Recognizers' and a section for 'Card Lengths'.

Num	Name	Field A	Field B	Field C
1	NCC Wiegand 26	0	0	256
2	NCC Ademco Wiegand 34	0	0	256
3	NCC Dorado EMPIII 34	0	0	0
4	Bit Image of Specified Length	0	0	0

Below the table is the 'Card Lengths' section with the following settings:

- Weigand Card Bits: 26
- Proximity Card Bits: 34
- Magnetic Strip Card Bits: 26
- Keypad PIN Digits: 4

At the bottom right of the window are buttons for 'OK', 'Cancel', and 'Help'.

### Card recognizer information

These fields display information about the access card formats that are currently supported by your access system. These fields generally need not be changed.

## ***Card lengths***

**Weigand Card Bits** - This is the number of bits that are used by Weigand card readers in the PassPoint system. Setting this field to 255 automatically allows the system to use any card which has a length greater than 26 bits. Note that if a varying card length (the setting of 255) is not required, you should set this field to the exact card length required by your installation.

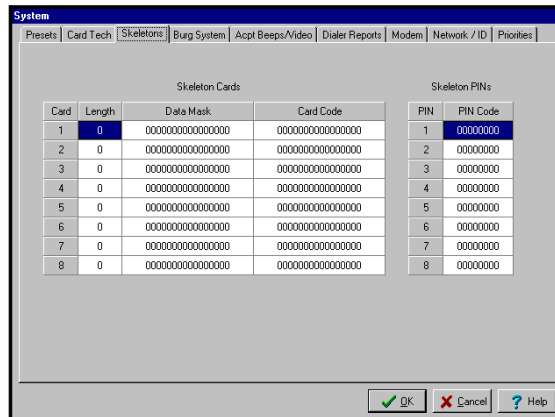
**Proximity Card Bits** - This is the number of bits that are used by Proximity card readers in the PassPoint system. Setting this field to 255 automatically allows the system to use any card which has a length greater than 26 bits. Note that if a varying card length (the setting of 255) is not required, you should set this field to the exact card length required by your installation.

**Magnetic Stripe Card Bits** - This is the number of bits that are used by Magnetic Stripe card readers in the PassPoint system. Setting this field to 255 automatically allows the system to use any card with a length greater than 26 bits. Note that if a varying card length (the setting of 255) is not required, you should set this field to the exact card length required by your installation.

**Keypad PIN Length** - This field can be set from three Personal Identification Number (PIN) digits to eight digits. This means that if you use 4 PIN digits, the first THREE digits of every PIN number assigned in the system MUST be unique. Also, the last digit assigned in the PIN numbers MUST NOT be ZERO. PIN numbers ending in zero are assumed to be duress PINs by the system.

## ***Skeleton codes (Skel tab)***

This screen allows the installer to edit the system's Skeleton Cards and Skeleton PINs:



Skeleton codes are used to unlock Access Points during Reduced Capability Mode (RCM) operation. They are used only when the communications link between the MLB and its DCM has been severed. Under these conditions, the DCM uses these skeleton codes as a very small card database. This database is used only when the communication link is down. When the communication link is restored, the skeleton code database is no longer utilized. RCM operation is also in effect when the system is downloading.

Skeleton codes come in two types: skeleton *cards* and skeleton *PINs*. The one that you choose depends on the type of entry readers your system uses. If your installation uses combination readers, and you have set them to grant access only after both a card swipe and PIN entry, only the card swipe will be read while the system is in RCM.

You can have up to eight skeleton cards and ten skeleton PINs.

## ***Assigning skeleton card codes***

Skeleton card codes work somewhat differently from skeleton PIN codes. There are eight skeleton card codes, but since skeleton card masks can be set up as filters, each skeleton card description can stand-in for many cards.

### ***Setting up a skeleton card to filter acceptable cards***

When you want a skeleton card to filter acceptable cards, imagine that the Card Data Mask is a strainer (the filter) and that the Resulting Card Code is a final test to see what made it through the strainer. The operations that occur on the card number require you to understand hexadecimal and binary arithmetic, and Boolean AND operations.

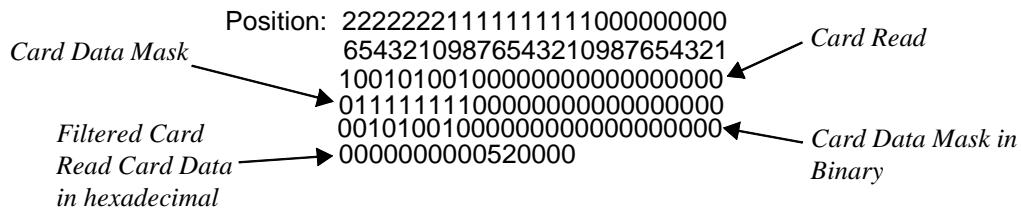
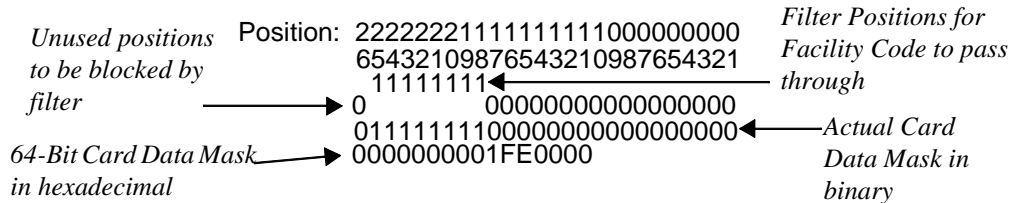
When a card is read by the access point in RCM, it will be passed through the Card Data Mask filter. The resulting value will be checked against the Resulting Card Code. An EXACT match of the Resulting Card Code will be accepted by the access point.

As an example, let's assume that we want all cards with the embedded Facility Code of 41 (decimal) to pass through access points. The cards used in your facility are 26-bit cards in this example. For this card format, the Facility Code is encoded into eight bits, starting with the 25th bit of a 26-bit card....

Position: 222222211111111100000000  
65432109876543210987654321  
|-----| ← Facility Code, in binary

Since you want to look at the Facility Code of all cards that are detected by the access point's readers, you want to check that all of the card's bits in the region of the Facility Code pass through the filter. Also, you want the EXACT match of the Facility Code in order to accept the card. You would then set up the skeleton card like this....

Lower 26 bits of Card Data Mask (all upper bits are 0's):



Length	Card Data Mask	Resulting Card Code
026	000000001FE0000	000000000520000

**Setting up a skeleton card to look for an exact match**

When you want a skeleton card to be an exact match, you must enter the same number in the Card Data Mask and the Resulting Card Code. As an example, if a 26 bit card whose number is, in hexadecimal, 02e60013, you should enter the data as....

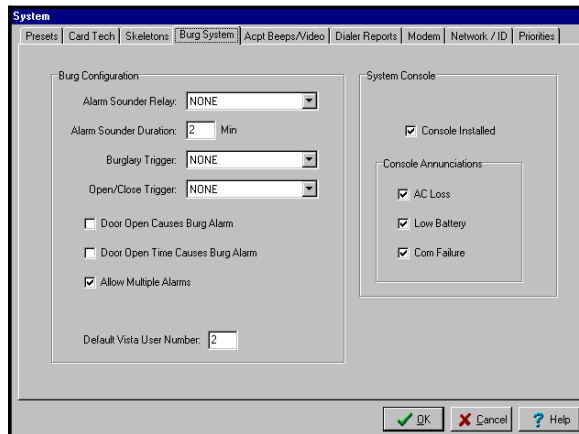
Length	Card Data Mask	Resulting Card Code
026	00000000FFFF0013	0000000002E60013

**Skeleton PIN codes**

Enter up to eight left-justified PIN codes that can be used as Skeleton PINs. The function performed by these PINs during RCM can be set for each individual Access Point in the DCM configuration screen.

**Burglary system options (Burg System tab)**

This screen allows some general burglary system configuration options to be set:





## **Burg configuration**

**Alarm Sounder Relay** - Enter the global relay number of the uncommitted relay you want used as a burglary alarm bell output. The indicated relay can only be operated by the burglary system within the PassPoint system. The relay must be globally assigned before it can be selected in this area.

**Alarm Sounder Duration** - This is the amount of time (in minutes) that the Alarm Sounder Relay will activate in response to a burglary condition. The alarm bell can be silenced by issuing a *Disarm* command while the bell sounds. The alarm bell will turn off automatically after this time expires.

**Burglary Trigger** - Enter the global trigger number of the uncommitted trigger you want used as a Burglary Trigger indicator. The indicated trigger can only be operated by the burglary system within the PassPoint system. This trigger can be used to notify the Long Range Radio system of a burglary condition. The trigger must be globally assigned before it can be selected in this area.

The Burglary Trigger will be on when there are no pending alarms. Electrically, the trigger will be drawing current; that is, it will measure as a logical low if it is measured with a Voltmeter when a pull-up resistor is used.

The Burglary Trigger will be off when there is a pending alarm. Electrically, the trigger will not be drawing current; that is, it will measure as a logical high if it is measured with a Voltmeter when a pull-up resistor is used.

**Open/Close Trigger** - Enter the global trigger number of the uncommitted trigger you want used as an Open/Close Trigger indicator. The indicated trigger can only be operated by the

burglary system within the PassPoint system. This trigger cannot be controlled manually because it is intended to electronically notify a foreign system of the Armed (Closed) or Disarmed (Open) arming condition of the burglary system of the PassPoint. This trigger can be used to notify the Ademco Long Range Radio system of a burglary condition. The trigger must be globally assigned before it can be selected in this area.

The Open/Close Trigger will be on when the system is Armed Away or Stay. Electrically, the trigger will be drawing current; that is, it will measure as a logical low if it is measured with a Voltmeter when a pull-up resistor is used.

The Open/Close Trigger will be off when the system is Disarmed. Electrically, the trigger will not be drawing current; that is, it will measure as a logical high if it is measured with a Voltmeter when a pull-up resistor is used.

**Door Open Causes Burg Alarm** - Check this box if you want Access Control Door Open Alarms to initiate a burglary alarm response. If you check this box, the selected burglary Alarm Bell Relay will turn on for the Alarm Sounder Duration.

**Door Open Timeout Causes Burg Alarm** - Check this box if you want Door Open Timeout Alarms to initiate a burglary alarm response. If you check this box, the selected burglary alarm bell relay will turn on for the Alarm Sounder Duration.

**Allow Multiple Alarms** - Check this box if you want successive alarm conditions on the same access point or zone to initiate a Burglary Alarm Response each time the condition occurs within a single arming period. If you do not check this box, each access point or zone will only be able to generate one alarm during a single arming period.

**Default Vista User Number** - Since all actions on a connected Vista alarm panel get logged to the Vista's event history log, any action that the PassPoint system initiates on the Vista panel needs to map to a Vista user number. The Vista user number indicated in this field will be associated with any Vista action that is induced by the PassPoint system.

### ***System console***

**Console Installed** - Check this box if you have wired an Ademco 6139 keypad to the system MLB for use as a system keypad. Make sure that this box is not checked if a keypad is not installed.

### ***Console annunciations***

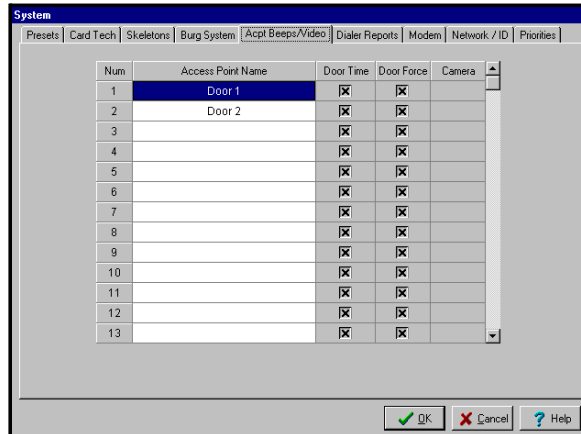
**AC Loss** - Check this box if the system keypad should sound slow beeps if ANY module in the PassPoint system loses AC power.

**Low Battery** - Check this box if the system keypad should sound slow beeps if ANY module in the PassPoint system experiences a low battery condition.

**Com Failure** - Check this box if the system keypad should sound slow beeps if a communications error occurs between the system's MLB and ANY module in the PassPoint system.

## ***Access point beeps and video (Acpt Beep/Video tab)***

This tab allows the selection of annunciation options for the system keypad as well as indication of which Access Points have been fitted with a video camera.



Each Access Point will be listed. Set the selection boxes in the appropriate column in order to indicate the Access Points that need to sound Door Open Alarms and Door Open Timeouts. If your PC has a supported video capture card, the column indicating video camera call-up will be enabled. If you want an Access Point to call up a live video screen when a visual verification is in process and you have a video camera pointed at the Access Point, set the appropriate selection box.

The beep mode is fast for Access Point Open Alarms, and slow for Access Point Timeout Alarms.



You can only make selections in the *Camera* column when you have the appropriate equipment installed.

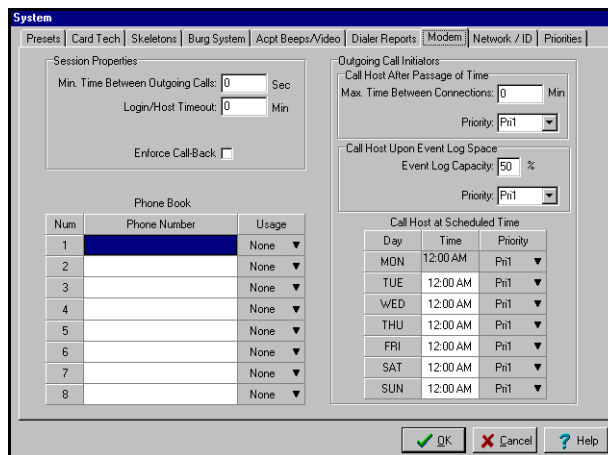
### ***Dialer reporting options (Dialer Reports tab)***

This screen allows the enable/disable selections for some of the possible Contact ID-formatted dialer messages that can be sent to a burglary Central Monitoring Station. Event types marked

by a check will be communicated to the Central Station by the VGM or a connected VISTA panel. This screen only pertains to systems that are using a VGM.

## Modem options (Modem tab)

This screen allows the configuration of communication connection and session options:



### Session properties

**Min Time Between Outgoing Calls** - This is the number of seconds that will be enforced between outgoing calls made by the PassPoint system. This setting allows a window of time when someone may call in to the PassPoint system, even when the system is busy making outgoing calls. This time only pertains to the interval between outgoing calls being made for different reasons. This time will not affect the interval between unsuccessful outgoing call attempts.

**Login/Host Timeout** - This is the amount of time (in minutes) that may expire after making a dial-in or dial-out connection. It is also the amount of time that, when expired, will force a re-negotiation of a connection with a PC Host System (in a future version of the product). When using a remote connection, if this timeout time passes without someone logging in, the system will terminate the connection by hanging up. Setting this field to 0 disables this timeout.



---

It is important to set this field to a non-0 value if using a modem connection. Do not set this field to a non-0 value if using a local connection.

---

**Enforce Call-Back** - Setting this option to (Y)es forces the PassPoint system to hang up on a call-in and automatically call back a predetermined phone number. This allows for a higher-security system since any dial-in that is answered by the PassPoint will terminate and the system will initiate a call to a known-safe phone number.

### ***Phone book***

The Phone Book is used to identify eight possible phone numbers through which the PassPoint system can contact a remote PC. These numbers do not need to be filled in if the only PC used to manage the system is directly connected to the system.

The usage settings specify the number that is used under a certain circumstance. One number should be selected to be used as call-back if the *Enforce Call-Back* option is selected. This is the number that the PassPoint system will call after a call-in is received.

All other numbers are used to dial a particular PC upon the occurrence of an event of a particular priority threshold. This allows the system to call different hosts to handle different types of events. This feature of the Phone Book will be best served by the upcoming Windows software.

## ***Outgoing call initiators***

### **Call host after passage of time**

If the indicated number of minutes passes without the system generating any remote connections, the system will initiate an outgoing call to the appropriate phone number based on the priority given to this event.

### **Event log capacity and priority**

When the Event Log capacity reaches the indicated percentage, the system will generate an outgoing call of the indicated priority.

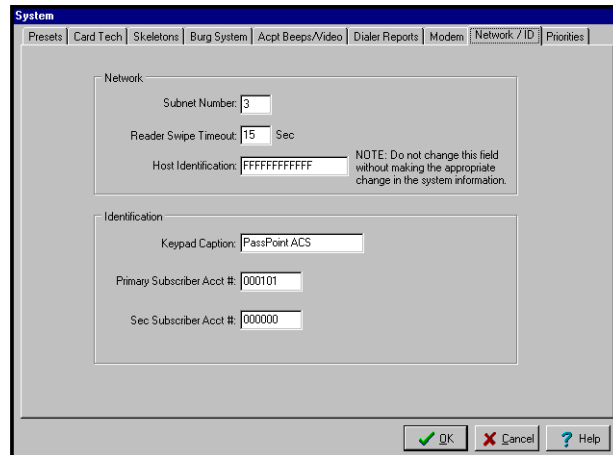
### **Call host at scheduled time**

The PassPoint system will initiate a call-out of the indicated priority at the indicated time on the selected day(s). Make sure that you completely specify the time in 12-hour format, indicating A.M. or P.M.

## ***Network ID options (Network/ID tab)***

This screen provides the settings for special network parameters and system identification information:





## Network

**Subnet Number** - This number, ranging from 1 to 255, selects a common grouping of network modules. In most cases, this number **SHOULD NOT BE CHANGED**. This number should only be changed if necessary when utilizing the same twisted pair wiring for the PassPoint system and other Echelon LonWorks-compatible devices. Contact Ademco for more details.

**Reader Swipe Timeout** - This is the number of seconds that a DCM or CPM reader interface will wait after a card is swiped or a PIN is entered. Under normal circumstances, the MLB will respond to the module to generate a grant or denial. However, if the MLB does not respond within the specified amount of time, the reader interface will reset. The default setting is 3 seconds. This default setting should be set higher if you are doing visual verification.

**Host ID** - This 12 hexadecimal digit number is used to validate a connection with the PassPoint *Express* software. The number

set here **MUST** match the number set for the PC software in order for uploads/downloads and event capturing to operate.

Although the Host ID has an initial value of “FFFFFFFFFFFF,” it should be changed by the installer to a unique value for security reasons.

### ***Identification***

**Keypad Caption** - This is the character string that is displayed on the top line of the system's 6139 keypad.

**Primary Subscriber Account Number** - The first four digits of this number will be sent to your primary central station monitoring service in the event that a call to the central station is warranted. The last two numbers represent the MLB number. This field cannot be edited because it is filled in automatically upon account database creation.

**Secondary Subscriber Account Number** - Enter in the secondary account number for this account. The first four digits of this number will be sent to your secondary central station monitoring service in the event that a call to the central station is warranted, and the primary central station is not responding. The last two numbers represent the MLB number.

## ***Priority options (Priorities tab)***

This screen displays the settings for the priority of all of the events that a PassPoint system can generate. The priority settings range from None through Priority Level 5. Events that have been set to a priority level of None will not be logged to event history. Priority Level 1 events are the lowest priority events that can be logged. Priority Level 5 events are the highest priority events that are logged. Any event that has been set to a Priority Level of None cannot be used as the trigger for an Event-Action relationship since the event is not being logged. Note that when transferring events to the host, the field panel MLB will transmit the oldest, highest priority events in the Event Log first, working down to lowest priority, most recent events.

You should keep in mind that these priority settings can affect remote connections. Altering the event priorities can cause outgoing calls to the host to be made, and can prevent events from being logged.



Chapter

# 11

## *Performing Access Point Functions*

Access functions allow you to control and regulate the Access Points of your premises. In this chapter you will learn how to:

- **Display and alter the status of Access Points and readers**
- **Change the system's threat level**
- **Control the system's anti-passback features.**

## ***What Are Access Point Functions?***

Access functions are those system functions that allow you to control and regulate your premises' Access Points and access groups. They include such things as bypassing or locking an Access Point. They also include things like controlling your system's ID readers and changing your system's threat level.

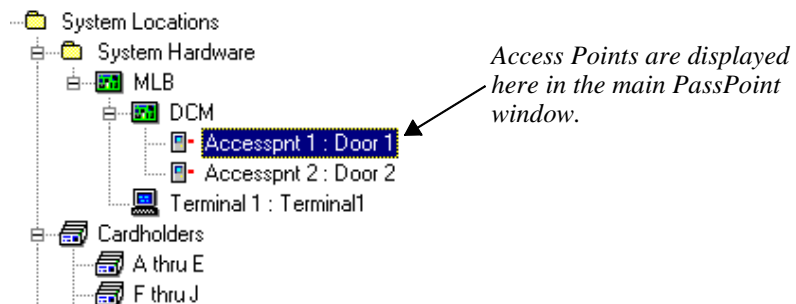
As you are using PassPoint, there will be many times when you will need to manipulate your Access Points. You will need to bypass, lock and protect Access Points. You will also need to configure Anti-Passback for your Access Points, tell the system when to grant access, and when to clear precedence levels. All of these functions are described in this chapter.

### ***Who performs these functions?***

Generally speaking, access functions are tasks that are performed after the system is installed and configured. These are the day-to-day operations that allow you to keep the system functioning properly. These tasks are not performed by the installer of the system (although they could be), but are performed by system Masters, Managers and Operators, since these are the people who are going to be using the system once it is installed and configured.

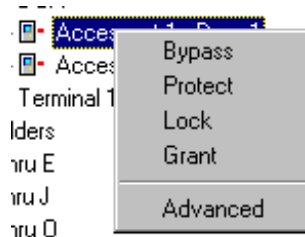
## Displaying and controlling Access Points

The first step in working with your Access Points is to display them on-screen. Access Points, like all system resources, are displayed in the main PassPoint window, along with their applicable DCM:



### **Right-click on an Access Point for options**

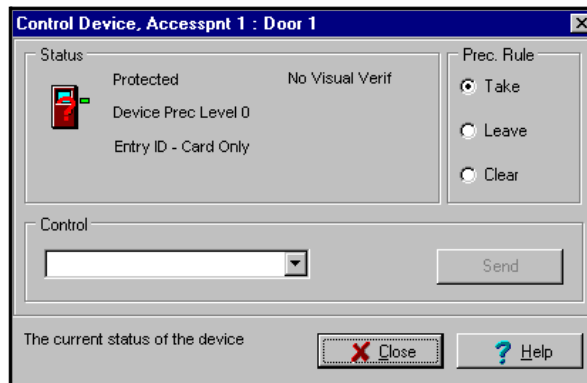
To control or view information about an Access Point, right-click on it. Right-clicking on an Access Point brings up a menu of options:



The options on this menu allow you to perform various access functions. From here you can *Bypass*, *Protect*, *Lock*, or *Grant* access to an Access Point. You can also call up a dialog box of “advanced” options.

## ***The Advanced menu option***

The *Advanced* option calls up a dialog box displaying information about the Access Point. It also lets you perform more tailored access functions than do the other menu options:



The dialog box is divided into three areas:

### ***Status***

This area shows the status of the selected resource. It is only updated upon initial display and when commands are sent from the *Control* area of the dialog box.

### ***Control***

This drop-down list contains the commands that pertain to the selected Access Point. Based on your selection, a *Send* button becomes visible or a *More* button becomes visible. *More* denotes that more data is needed, so clicking the *More* button will cause a second dialog box to be displayed, allowing you to enter the extra parameters. From either dialog box, clicking the *Send* button will then “send” the selected command to the MLB, updating the Status area.



*For example, if you want to bypass an Access Point, you can simply select Bypass from the menu. In this case the Access Point will be bypassed until you Protect it again. However, if you want to set a special time limit for the bypass, you can use the Bypass option in the Control section of the Advanced dialog box. This will let you choose a length of time for the Access Point to be bypassed.*



---

The bypassing and granting access functions provide periods when the access point will be unprotected.

---

## **Locking Access Points**

Locking Access Points means keeping them from being opened, even by valid access cards/Cardholders. Also, a locked Access Point can be returned to normal operating status only by *Protecting* it after it has been locked.

To lock Access Points:

- 1. In the main PassPoint window, right-click on the Access Point you want to lock.**
- 2. Select *Lock* from the menu.**

The Access Point you selected will be locked. The message “ACCPT LOCK” will appear in red in the status bar at the bottom of the screen, indicating the current condition of the Access Point.

---

## ***Protecting Access Points***

Protecting Access Points simply means returning them to a normal operating status. When an Access Point is protected, only valid Cardholders can access it. You choose the *Protect* option when you want to change an Access Point from locked, bypassed, or exit only.

To protect an Access Point:

- 1. In the main PassPoint window, right-click on the Access Point you want to protect.**
- 2. Select *Protect* from the menu.**

The Access Point you selected will be protected.

There is no special status message to indicate that an Access Point is protected, since that is the normal operating mode. The message "SYSTEM NORMAL" will continue to be displayed.

## ***Bypassing Access Points***

When an Access Point is bypassed, the locking mechanism of the door is disabled, leaving it free to be opened without the need for card identification. The system will not see these entries and exits as a problem, since it knows the Access Point has been bypassed. To the system, it's as if a bypassed Access Point is to be ignored.

To bypass Access Points:

- 1. In the main PassPoint window, right-click on the Access**

**Point you want to bypass.**

**2. Select *Bypass* from the menu.**

The amount of time that the Access Point will be bypassed is set in the Edit System Administration Options screen. This value can only be set by Installer level users.

***Timed bypass***

If you want to bypass the Access Point for a specific amount of time (other than the global system bypass time):

**1. In the main PassPoint window, right-click on the Access Point you want to bypass.**

**2. Select *Advanced* from the menu.**

The Advanced options dialog box appears.

**3. In the *Control* section of the dialog box, select *Bypass Timed*.**

This will allow you to set a specific amount of time for the Access Point to remain bypassed.

**3. Click *More*.**

A dialog box will appear, allowing you to enter a length of time for the bypass (2 - 65535 minutes).

**4. Enter a bypass time, then click *Send*.**

The Access Point you selected will be bypassed for the length of time you entered. Once that time has elapsed, the Access Point will return to a *Protected* state.

---

## **Granting access to Access Points**

Typically, when a Cardholder presents his/her ID card to a reader, he/she is granted access to the Access Point if they have rights to do so. However, there will be times when you will want to grant access to certain Cardholders who have lost their cards, do not have rights to an Access Point, etc. In these cases, you can use the system's Grant Access function.

### **Granting access can be done in two ways**

You can grant access in two different ways:

- **Grant**

This method unlocks the Access Point according to the Access Point's normal configuration timing. That is, if the Access Point has been configured to unlock for five seconds when a valid card is presented to it, the grant command will unlock the Access Point for five seconds. At the end of five seconds, the Access Point will lock and continue operating normally.

- **Grant with special timing**

This method allows you to choose how long you want the door to remain open. It also lets you select how long the door can remain open when an alarm occurs. This method is useful if you need to let a group of people through an Access Point.

- 1. In the main PassPoint window, right-click on the Access Point to which you want to grant access.**

- 2. Select *Grant* from the menu.**

The system will grant access to the Access Point. The Access Point will unlock and then relatch according to its

normal configuration.

***Grant with special timing***

If you want to grant access to the Access Point with special timing:

- 1. In the main PassPoint window, right-click on the Access Point.**
- 2. Select *Advanced* from the menu.**

The Advanced options dialog box appears.

- 3. In the *Control* section of the dialog box, select *Grant with special timing*.**
- 4. Click *More*.**

A dialog box will appear, allowing you to enter time parameters for the grant:

**Unlock Time** - Enter the time (1-65535 seconds) during which the door control relay is energized, unlatching the door.

**Time Open** - In this field, enter the time (1-65535 seconds) that the Access Point's door can remain open before a violation occurs. When a violation does occur, the DCM will inform the system of the situation, allowing you to take appropriate steps. This field is only valid if Door Status Monitoring is configured for the Access Point.

The value in this field must be greater than or equal to the *Unlock Time*.

**P-A Time** - In this field, specify the time of the pre-alarm signal. When an the Access Point is returned to Protect mode, the pre-alarm signal is activated and the door is left unlatched until the time has expired, whereupon the door re-

latches and the pre-alarm signal ceases. The value of pre-alarm time can range from 1 to 65,535 seconds (18.2 hours). This field is only valid if Door Status Monitoring and pre-alarm triggering is configured for the Access Point.

The value in this field must be less than or equal to the *Time Open*.

5. Click *Send*.

## ***Shunting and unshunting Access Points***

When an Access Point is shunted, the condition of the Door Status Monitoring zone (if there is one) is basically ignored. Door open alarms and door open timeout alarms can no longer be generated, and the DCM operates the Access Point as though there is no DSM zone assigned to it. This allows a door with a faulty DSM switch to continue to provide service in a semi-protected way, until the DSM switch can be repaired.



---

Since shunting an access point defeats the DSM for that door, the system will not be able to recognize when a door has been forced open while it is shunted.

---

To shunt (or unshunt) an Access Point:

1. **In the main PassPoint window, right-click on the applicable Access Point.**
2. **Select *Advanced* from the menu.**

The Advanced options dialog box appears.
3. **In the *Control* section of the dialog box, select *Shunt DSM Zone* or *Unshunt DSM Zone*.**

#### **4. Click Send.**

The Access Point you selected will be shunted/unshunted.

### ***Choosing an identification method***

Each Access Point has an identification reader. It might be a card reader, a PIN reader, or a combination reader, meaning that it has both card and PIN capability. If an Access Point uses a card only or PIN only reader, the choice of identification mode is obvious. But if you are using combination units at any of your Access Points, you might want to customize the identification method.

*For example, if you are using a combination card/PIN reader at a relatively unimportant Access Point, you might want to set the reader to accept either cards or PINs in order to grant access. Or, if the Access Point leads to a very secure area, you might want to set the reader to accept only cards and PINs before access is granted. You might even want to set the order in which these identification methods are presented.*

#### ***You can choose from five identification methods***

When selecting the identification method for your Access Points, the system will allow you to select one of five options:

- **Card only**
- **PIN only**
- **Card followed by PIN**
- **PIN followed by Card**
- **Card or PIN**

Additionally, you can configure these identification methods for entry or exit use, depending how your Access Point is set up. For instance, you would need an exit reader to configure an exit identification method.

To configure the identification method for an Access Point:

**1. In the main PassPoint window, right-click on the applicable Access Point.**

**2. Select *Advanced* from the menu.**

The Advanced options dialog box appears.

**3. In the *Control* section of the dialog box, select *I.D. Modes (Entry)* or *I.D. Modes (Exit)*.**

**4. Click *More*.**

A dialog box will appear, allowing you to choose entry or exit ID mode for the Access Point.

**5. Click *Send*.**

The identification method you've selected will be applied to the Access Point. The status area will change to indicate the new identification method.

## ***Setting Access Points as Exit Only***

When you set an Access Point to Exit Only, the system will deny all entry requests to the Access Point, but will honor exit requests. The entry reader associated with the Access Point is disabled. Also, no "Access Request" or "Access Denied" events will be logged for the Access Point.

To set Access Points to Exit Only:



1. **In the main PassPoint window, right-click on the applicable Access Point.**
2. **Select *Advanced* from the menu.**  
The Advanced options dialog box appears.
3. **In the *Control* section of the dialog box, select *Exit Only*.**
4. **Click *Send*.**

The Access Point you selected will be set in the Exit Only mode. The message “EXIT ONLY” will appear in red in the status area at the bottom of the screen, indicating the current condition of the Access Point.

## ***Configuring Visual Identification***



The Visual Identification features of the PassPoint system have not been tested for UL compliance.

In order to add extra security to Access Points, the system provides a Visual Identification mode. When selected, this option requires the system to defer to an operator to visually identify all Cardholders after a Cardholder’s card/PIN has already been verified by the system.

Visual identification occurs at the user terminal and is performed by a system operator. Once the Cardholder’s card/PIN is accepted by the system, the user terminal will display the Cardholder’s name, requiring the operator to positively identify the Cardholder before access is granted.



---

If there is no system operator logged in and Visual Verification is turned on, the system will automatically deny any access requests. A message will be logged in the Event Log describing this denial (“Visual Verification, No Login”).

---

To configure Visual Identification for an Access Point:

1. **In the main PassPoint window, right-click on the applicable Access Point.**
2. **Select *Advanced* from the menu.**

The Advanced options dialog box appears.

3. **In the *Control* section of the dialog box, select *Visual Verification mode*.**
4. **Click *More*.**

A dialog box will appear, allowing you to choose the user terminal you want to use for visual identification with the applicable Access Point.

5. **Make your choice and click *Send*.**

## ***Clearing the precedence level of an Access Point***

Precedence levels determine when certain actions may take place on system resources. For example, an Access Point may have a precedence level of 3. Unless an operator also has a precedence level of 3 or higher, he/she will not be able to bypass, lock, or do anything else to the Access Point.

There are two Access Point commands you should be aware of, both of which let you reset the precedence level of an Access Point. They are:

- **Clear Precedence**

This command simply returns the precedence level of the Access Point to 0. It does not analyze the system's schedules to determine what the current state of the Access

Point should be (i.e., locked, bypassed, etc.).

- **Resume as scheduled**

This command returns the precedence level of the Access Point to the precedence level of the last schedule to affect it. When this command is issued, the system analyzes all the schedules that directly affect the Access Point. After the schedules are analyzed, the system will determine what state the Access Point should be in.

For instance, the schedules may indicate that the Access Point should currently be bypassed. If the schedule has a precedence level high enough to affect the Access Point, the Access Point will take on the schedule's precedence level.

Both of these commands are accessed from the Advanced options dialog box and can be issued at any time.

## ***Anti-Passback***

Each Access Point can be configured to operate with the system's Anti-Passback feature. Anti-Passback is used to prevent occupants from using their card at an Access Point and handing it back through the doorway to an unauthorized individual, who would then use the same card to obtain entry or egress through the same Access Point.

Anti-Passback is a real-time programmable feature for each Access Point. When enabled, the number of minutes that must transpire between "successful" access attempts is programmable as a global value. This means that there is one programmable number of minutes which is used by all Anti-Passback Access Points. This time defines how long the system will wait before it allows the same card to be used at the same Access

Point card reader.



---

The global Anti-Passback time is set in the Edit System Administration Options screen. This value can only be set by Installer level users.

---



---

Anti-Passback functions are automatically disabled each time the panel exits programming (i.e., Reduced Capability Mode).

---

***There are three Anti-Passback options***

When setting Anti-Passback for your Access Points, the system will allow you to select one of three options:

- **None**

There is no restriction as to the passage of a specified length of time that must transpire between entry attempts or exit attempts at a single Access Point.

- **Soft**

Anti-Passback restrictions are in effect. Upon the occurrence of an Anti-Passback violation, the system will grant access (if all access requirements are satisfied). However, a Soft Anti-Passback Violation event will be logged in the system's Event Log.

- **Hard**

Anti-Passback restrictions are in effect. Upon the occurrence of an Anti-Passback violation, the system will deny access (regardless of the usual access requirements) and will log an Access Denial event with a reason code of Hard Anti-Passback Violation in the system's Event Log.

## **Configuring Anti-Passback**

To configure Anti-Passback for an Access Point:

**1. In the main PassPoint window, right-click on the applicable Access Point.**

**2. Select *Advanced* from the menu.**

The Advanced options dialog box appears.

**3. In the *Control* section of the dialog box, select *Anti-Passback mode*.**

**4. Click *More*.**

A dialog box will appear, allowing you to choose an Anti-Passback mode for the Access Point (None, Hard, or Soft).

**5. Make your choice and click *Send*.**

The Anti-Passback setting you have selected will be applied to the Access Point.

## **Forgiving Anti-Passback**

So far you have seen how to apply Anti-Passback to Access Points. You can, however, elect to temporarily “forgive” anti-passback for a specific Access Point or for all Access Points without having to go back into the Access Point configuration screens and change their settings. You can also forgive Anti-Passback for a specific Cardholder.

### ***Forgiving Anti-Passback for an Access Point***

When you forgive Anti-Passback for an Access Point, the system erases all of its recent Anti-Passback data for the Access Point. This means that anyone who passed through the door

within the Anti-Passback time will now be able to come in again, even though the Anti-Passback time has not expired for them.

For example, if you have set the front door of your building with an Anti-Passback time of ten minutes, people passing through the front door will have to wait ten minutes before they can enter through the front door again. However, if you forgive Anti-Passback for the door, anyone who came through the door within the last ten minutes will be able to pass through it again.



---

Forgiving Anti-Passback for an Access Point does not change the Access Point's Anti-Passback setting. The setting for the Access Point remains the same. It simply allows those who passed through within the Anti-Passback time to enter again.

---

To forgive Anti-Passback for one Access Point, follow the procedure below:

**1. From the *Control* menu, select *Forgive APB>Access Point*.**

A dialog box appears, in which you can select the applicable Access Point for which to forgive Anti-Passback.

**2. Make your selection and click *Send*.**

The system will forgive the Anti-Passbacks for the specified Access Point only.

## ***Forgiving Anti-Passback for a Cardholder***

To forgive Anti-Passback for a Cardholder, follow the procedure below:

**1. From the *Control* menu, select *Forgive APB>Cardholder*.**

A dialog box appears, in which you can select the applicable Cardholder for which to forgive Anti-Passback.

**2. Make your selection and click *Send*.**

The system will forgive the Anti-Passbacks for the specified Cardholder only.

## ***Threat Levels***

With PassPoint, a global condition can be set by system operators that can be used to qualify a “state of emergency.” This global condition is called a *Threat Level*.

PassPoint supports six Threat Levels, TL0 through TL5. TL0 is considered normal operation. It is also the default setting. TL5 is the highest Threat Level.

When you configured your access groups, you were asked to apply a “Maximum Threat Level” to each group. This is the maximum threat level under which (and including) the group is valid. If the Threat Level is above the one indicated by the access group, the access group will not qualify as valid. This feature is useful in locations where, under emergency conditions, occupants must be routed through a pre-determined set of Access Points.

For example, each occupant can be made a member of a “normal” access group and an “emergency” access group.

When the Threat Level is elevated, the “normal” access group would then be invalid, forcing the occupant to utilize a different set of Access Points and schedules as specified by the “emergency” access group.

“Threats” are defined by the installer and the facility in which the system is installed. For instance, if the facility is a chemical plant, a threat might be a chemical spill. In an oil refinery, a threat might be a fire or an explosion. It is up to the installer to determine what the possible threats are for the facility, and what Threat Level to assign to each threat.

Also, it is not necessary to use all six Threat Levels in a facility. You can use one, two, or no Threat Levels. If the facility has no use for Threat Levels, you can simply leave the default values.

### ***Changing the Threat Level***

You can change the system’s default Threat Level at any time (provided that you have been granted this system privilege). To do so, follow the procedure below:

**1. From the *Control* menu, select *Threat Level*.**

The system will present a sub-menu of threat level choices, ranging from “None” to Threat Level “5.”

**2. Select the appropriate Threat Level from the sub-menu.**



---

Changing the threat level can alter the validity of Access Groups. Always make sure that occupants have a valid and usable path of egress from the premises.

---



Chapter

# 12

## *Uploading and Downloading the Database*

This chapter explains the basic use of the PassPoint database. In this chapter you will learn about:

- **System accounts; what they are and how they are used**
- **Uploading the system database**
- **Downloading the system database**

---

## ***What Is the Database?***

Each MLB in your system contains a database. The database contains all of the information your system needs to operate properly. Every time you make a change to your system's configuration, the data you have entered is stored in the database. Throughout this manual you have been seeing different types of configuration data, including schedules, access groups, etc. All of this information is stored directly within your system's MLB. Collectively, this information is referred to as the "database."

Obviously, the information in your database is critical. Without it, your system simply would not function. Therefore, it is essential that you be able to manage your database, not only so that you can back it up and keep it safe in case of hardware failure, but also so that you can view and print event reports that tell you how your system is performing.

### ***System accounts***

In order to make using your system's database efficient, PassPoint uses system *accounts*. Essentially, an account is a way of accessing a database on an MLB. Each MLB is assigned a specific account number. Then, when you want to access a database (for backing up, event viewing, etc.), you select the applicable account number.

Accounts help you manage the PassPoint system by treating each MLB as an independent unit. Each MLB is assigned a specific account number. Using this number, you can back up and restore the database for a specific MLB, view the Event Log for the MLB, generate reports, etc. For installers who use

PassPoint *Express* to administer multiple sites belonging to the same customer, a separate account should be set up for each site. This way, when you bring up PassPoint *Express*, you can select the account (i.e., site) you want to work with.

If the installation site has only one MLB, system accounts are still needed, because you cannot upload or download the database without an account. In this case, you will need to set up only one account.

### ***What information is in the account database?***

Each account database entry stores the configuration information for the equipment installed at that site. This includes hardware configuration, schedules, access groups, and all of the card database information. Essentially, this is all the information necessary to replicate the site's programming on a new MLB, should the first system become damaged.

In addition, all the uploaded event history is categorized by account, so that the event history is context-sensitive to the appropriate installation. When the user starts up PassPoint *Express*, it is important that the "context" of the particular account get loaded. In this way, PassPoint *Express* can load the appropriate account information before communicating with the equipment.

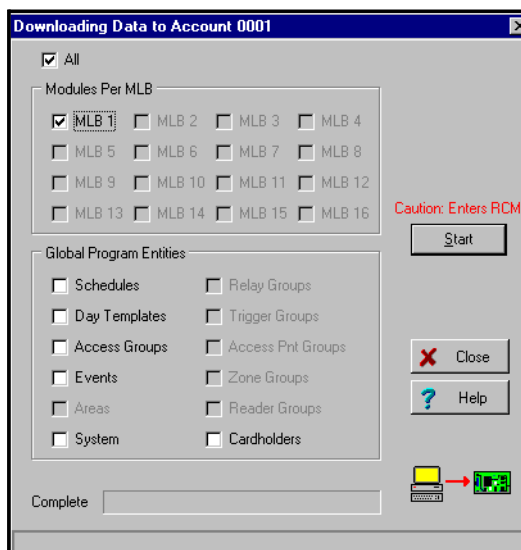
## Downloading the database

The Download feature is provided to allow the PC user to send to the MLB any database changes that have been made since the last download.

To download, follow the procedure below:

**1. From the *Config* menu, select *Download*.**

The Download dialog box appears:



The data to be downloaded is broken into several segments, any of which you may check to specify that you want to download that segment. Checking the “All” selection will override the other, individual selections and send all of the data segments to the MLB. By default, the segments which have been modified since the last download will come up selected when the dialog box is opened.



---

When the Cardholder information is selected for downloading, only those individual cardholder files which have been modified since the last downloaded will be sent to the MLB.

---

For an account recovery/re-creation (in the instance where the hardware was replaced and/or defaulted), you will select *All*. This will send down all of the system information to the MLB.

**2. Click *Start*.**

The download process will begin. This process may take as long as several minutes, depending on the size of the database and the number of segments being downloaded.

## ***Uploading the database***

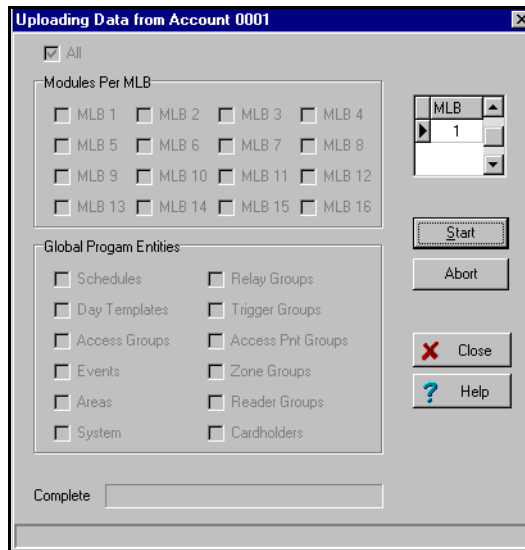
The Upload feature allows the PC user to create an account using an existing MLB installation as the basis for the account. All of the programming of the features on the MLB will be brought up to the currently loaded PassPoint *Express* account. Any settings in the currently loaded account will be completely over-ridden in favor of the new settings retrieved from the MLB. This means that any data which is not stored on the MLB will be lost for this account, including some resource names and much of the cardholder auxiliary information (Address, Picture, Notes, Custom Fields, etc.).

As a normal course of events, the Upload feature will not be used often. It should only be used in extreme cases where it is required that a new account be created by using the existing MLB programming.

To upload the database, follow the procedure below:

**1. From the *Config* menu, select *Upload*.**

The Upload dialog box appears:



The data to be uploaded is broken into several segments. For an upload, the only possible setting is *All*, since a partial upload would not be meaningful. Once the *Start* button is clicked, the *Abort* button is then activated and the upload begins.

**2. Click *Start*.**

The upload process will begin.

You may click the *Abort* button to cancel the upload at any time prior to the completion of the upload. After the upload is complete, the dialog box will automatically close and you will see the new system settings reflected in the account.

Chapter

# 13

## *Using PassPoint Reports*

Reports allow you to quickly view information about the configuration and operation of your PassPoint system. In this chapter you will learn:

- **About the different types of PassPoint reports**
- **How to use the Event Reporter to run system reports**

---

## ***PassPoint Reporting***

The PassPoint reporting tool allows you to quickly view configuration and operational information for your system. Basically, the reporting tools pulls up the data in the PassPoint database, allowing it to be displayed, printed, sorted and exported.

There are two kinds of reports: fixed and full query. Fixed reports are standard PassPoint reports that cannot be changed. Full query reports allow you to choose more specifically the type of data that will be displayed. When you select a full query report, the system calls up a “query builder,” a separate tool in which you choose the types of data you want displayed and the order in which you want it.

The table below lists each of the PassPoint reports, along with its type and a brief description:

Report Title	Type	Description
Access Groups	Fixed	Access Group Configuration
Access Point Activity	Full Query	All Access Point Related Events
Alarms	Full Query	Alarm Events Only (Access Point and Zones)
Burglary System Activity	Full Query	Burglary System Related Events
Card Denials	Full Query	Access and Egress Denials



Report Title	Type	Description
Card Related Events	Full Query	Events that pertain to Cardholders
Card Trace Events	Full Query	Card Trace Events
Cards (All)	Full Query	All CardHolders, Sorted by Last Name
Cards by Department	Full Query	All Cards, Sorted by Department
Cards in Access Group	Full Query	All Cards where Assigned Access Group = Supplied Acc Grp
Cards in Department	Full Query	All Cards in a Supplied Department
Day Templates	Fixed	Day Template Configuration
Event Actions	Fixed	Event Action Configuration
Events (All)	Full Query	All Events in Chronological Order
Events (In date range)	Full Query	All Events Within a Supplied Date Range
Exec Priv Cards	Full Query	All Executive Privilege Cards
Hardware Module Configuration	Fixed	Hardware Module Configuration
Manual Grants	Full Query	All Manual Access Grants
Operator Related Events	Full Query	All Events caused by Operator Actions

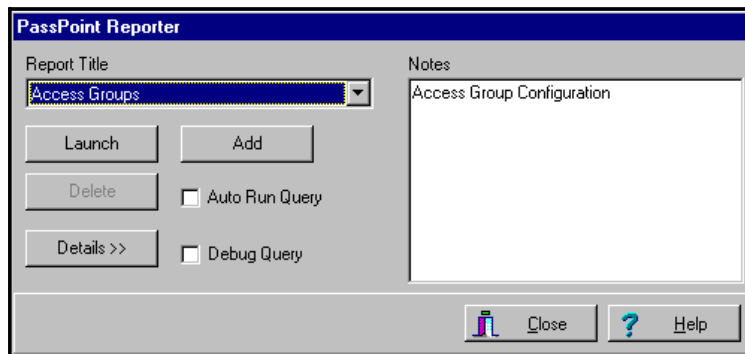
---

Report Title	Type	Description
Report List	Full Query	Available Reports
Schedules	Fixed	Schedule Configuration
System Wide Options	Fixed	System Wide Options Configuration
Time & Attendance	Full Query	Chronological Card Activity Within Date Range
Zone Activity	Full Query	Zone Related Events

All of events tools are run from the Event Reporter. When run, each report will give you detailed information about the PassPoint parameter you selected. For instance, running the Day Template report will provide you with detailed information about all of your system's Day Templates.

## Using the Event Reporter

The Event Reporter is the PassPoint tool used to run/view reports. To launch the Event Reporter, select *Reporting* from the *Tools* menu. The Event Reporter will appear:



The Event Reporter displays all of the available reports in a drop-down list box. To run a report, choose the applicable report, then click *Launch*. You may then need to choose additional parameters for the report before it actually launches.

Each of the fields and buttons of the Event Report are described below:

**Report Title** - The *Report Title* drop-down list allows a selection of the report type that you would like to run. When you make a selection from this list, the *Notes* field will display information about the report that you have selected.

**Notes** - The *Notes* field may display a brief description about the report selected in the *Report Title* field.

**Launch** - Clicking this button will bring up the Report Selection screen. Some of these reports will run automatically and open up into a large screen that will allow you to preview the data before you actually print it. Other reports may ask for information before running the report. Some reports will open up a large screen that will allow you to graphically describe the exact details of the report that you wish to run.

**Add** - Click button when you want to add a report to the *Report Title* list. Only reports that have been generated using the graphical report creator can be added to the *Report Title* list.

**Delete** - Click this button to delete a report in the *Report Title* list. You can only delete reports that you have created.

**Details** - Some of the reports in the *Report Title* list keep statistics such as last time and date when run. Click this button to display the report statistics. Once report statistics are

displayed, this button will change to a *Hide* button, which will close the statistic display.

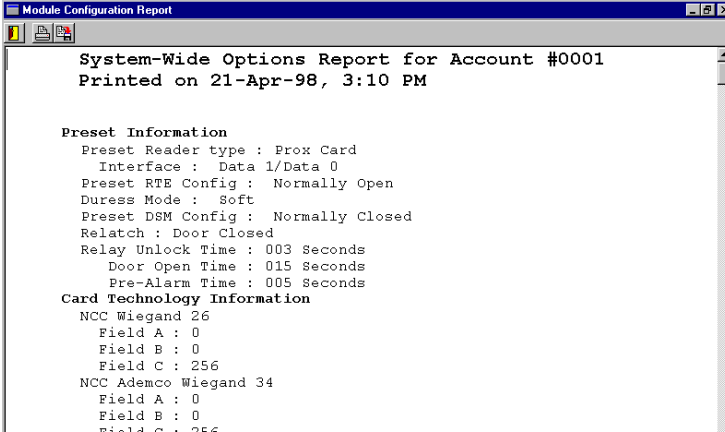
**Hide** - Some of the reports in the *Report Title* list keep statistics such as last time and date when run. Click this button to hide the report statistics. Once report statistics are hidden, this button will change to a *Display* button, which will close the statistic display.

**Close** - Click this button to close the Report screen.

## Viewing reports

Once you've launched a report, the system will search the database for all the applicable data, then display the report on-screen in a separate window.

If you've launched a fixed report, the window will look similar to the one below:



```
Module Configuration Report
System-Wide Options Report for Account #0001
Printed on 21-Apr-98, 3:10 PM

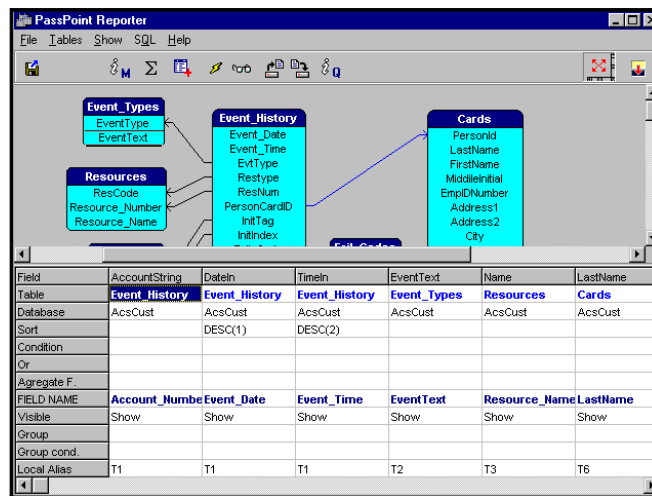
Preset Information
Preset Reader type : Prox Card
Interface : Data 1/Data 0
Preset RTE Config : Normally Open
Duress Mode : Soft
Preset DSM Config : Normally Closed
Relatch : Door Closed
Relay Unlock Time : 003 Seconds
Door Open Time : 015 Seconds
Pre-Alarm Time : 005 Seconds

Card Technology Information
NCC Wiegand 26
Field A : 0
Field B : 0
Field C : 256
NCC Ademco Wiegand 34
Field A : 0
Field B : 0
Field C : 256
```

As you can see, the report displays information about all of the modules currently enrolled in the system.

At the top of the screen is a tool bar. Using these toolbar buttons, you can exit the report, print the report, or save the report for future viewing.

If you've chosen a full query report, the query builder screen appears:



From here you can choose which data fields to display, then run the query.



## Appendix

# A

## *System Defaults*

Should your PassPoint system ever lose AC power without a battery backup or be intentionally powered down, there are a number of default settings that will take effect once power is restored to the system. These default settings apply to the operating parameters of the system that are not part of the configuration database (e.g., the state of relays). Database configuration (e.g., module configuration, modem configuration, etc.) will not be affected by a power loss and restart.

This appendix lists all of the default values that will be instituted upon power-up. These settings also take place each time system configuration information is downloaded and the system enters programming (RCM) mode.

Note that downloading schedules, cards and other ancillary data does not cause the system to enter programming mode. Only “installer-related” configuration options cause the system to enter programming mode.

---

## ***Default System Values***

The following default system values will be instituted whenever the PassPoint system loses power and is powered backup. Remember that a battery backup will keep you from losing the following program data should an AC loss situation occur.

Uncommitted Relays: Off, Enabled, Precedence Level 0

Uncommitted Triggers: Off, Enabled, Precedence Level 0

Uncommitted Readers: Enabled, Precedence Level 0

ID Mode: Card only for card reader  
PIN only for keypad  
Card+PIN for combination units

Uncommitted Zones: Unshunted, Protected, Precedence Level 0

Access Points: Protected, Precedence Level 0

DSM Zone: Unshunted

RTE Zone: Unshunted

Door Control: Relay Off

Pre-Alarm Trigger: Off

Entry ID Mode: Card only for card reader  
PIN only for keypad  
Card+PIN for combination units



Exit ID Mode:	Card only for card reader PIN only for keypad Card+PIN for combination units
Visual Verification:	Off
Anti-Passback Setting:	None
Access Groups:	Enabled
Cardholders:	All Forgiven, 1 Anti-Passback and Entry/Exit violation
Threat Level:	0
Burglary System:	Disarmed

---



The above settings may be overridden by schedules that are evaluated to be OPEN when the system “wakes up” from power-down. This is because schedules are evaluated upon system start-up, and the opening actions for OPEN schedules are performed.

---



## Appendix

# B

## *Keypad Messages*

The PassPoint system can use a standard Ademco 6139 alpha-numeric keypad to display system status and to annunciate trouble conditions such as door-open time-out alarms. If your system does contain a keypad, the following appendix lists all of the messages that the keypad might display while the system is in use.

Messages appearing on the keypad are not resource-specific. That is, they do not state which zone is in alarm, which Access Point is open, etc. If the keypad warns you about such a condition, you will need to refer to the applicable PassPoint *Express* screen to find out which resource is being reported on.



---

## ***Keypad Messages***

Following are all the keypad messages that may appear while the PassPoint system is in use:

SYSTEM NORMAL	All is well
LOCAL ONLINE	System operating locally
LOCAL OFFLINE	Local system out of contact with PC
REMOTE ONLINE	System operating via modem
REMOTE OFFLINE	Remote system out of contact with PC
ZONE TRBL	Zone(s) in trouble
ZONE SHNT	Zone(s) shunted
ZONE BYP	Zone(s) bypassed
ZONE ALARM	Zone(s) in alarm
RDR DIS	Reader(s) disabled
RLY DIS	Relay(s) disabled
RLY SUPV	Relay(s) failing supervision
ACCPT SHNT	Access point DSM(s) shunted
ACCPT BYP	Access point(s) bypassed
ACCPT LOCK	Access point(s) locked

ACCPT EXIT	Access point(s) in exit-only mode
ACCPT DO ALARM	Access point(s) in door-open alarm
ACCPT DOT ALARM	Access point(s) in door-open time-out alarm
ACCPT RLY SUPV	Access point's relay(s) failing supervision
ACCPT RTE TRB	Access point's RTE(s) in trouble
ACCPT DSM TRB	Access point's DSM(s) in trouble
TRIG DIS	Trigger(s) disabled
ARMED AWAY	Burglary system armed away
ARMED STAY	Burglary system armed stay
PROGRAM (RCM) MODE	System in Programming Mode, DCMs in Reduced Capability Mode
MOD COM FAIL	Communication failure to module(s)
MOD AC LOSS	AC loss at module(s)
MOD LOW BATT	Low battery at module(s)
DENY OVR	Deny Override set
MLB MDM FAIL	MLB unable to communicate with modem
AG DIS	Access group disabled
OPEN CKT	MLB getting no response from keypad



Appendix

C

## *Event Log Messages*

This appendix contains a complete listing of all PassPoint event log messages. The messages in this appendix have been arranged by type for easier reference.

## Event Log Messages

Configuration Setting Changes							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to CS?	Defaulted to Dial to CS?	Contact ID Code
USER LOG-IN:	Occurs when a User Logs in to Menu Mode	1		Yes			
USER LOG-OUT:	Occurs when a User Logs out of Menu Mode	1		Yes			
AUTO USER LOG-OUT:	The system automatically logged a user out due to the expiration of the allotted time without any user activity.	2		Yes			
PROG MODE ENTERED:	Occurs when the Installer enters Programming Mode and the remainder of the system enters Reduced Capability Mode	2		Yes	Yes	Yes	E429 Prog Mode Entry
PROG MODE EXIT:	Occurs when the Installer exits Programming Mode and the the system returns to normal operation	2		Yes	Yes	Yes	E430 Prog Mode Exit
SYSTEM DEFAULTS LOADED:	Occurs when the Installer reprograms the system to its factory default settings.	2		Yes	Yes	Yes	E306 Panel Prog Change
SYSTEM TIME SET:	Occurs when a User alters the Time Setting of the System	2		Yes	Yes	Yes	E625 Time Set
USER CODE EDITED:	Occurs when User Log-in Codes are altered	2		Yes			
DFLT CARD RECOG LOADED:	The Card Recognizer settings were defaulted by the Installer.	2		Yes			
VISTA I/F CONF EDITED:	Occurs when Installer alters Vista Panel Interface parameters	2		Yes			



<b>Configuration Setting Changes (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to CS?</b>	<b>Defaulted to Dial to CS?</b>	<b>Contact ID Code</b>
COMM PARAMETERS EDITED:	Occurs when Installer alters Modem Communications parameters	2		Yes			
NETWORK CONFIG EDITED:	Occurs when Installer alters the Network Configuration information	2		Yes			
FCLTY/SYS/KPD EDITED:	Occurs when Installer alters the System Identification information	2		Yes			
AUTHLVLPRIVS EDITED:	N/A this Revision, but will occur when the Card Holder Authority Level Privileges are altered	2		Yes			
MODULE LIST EDITED:	Occurs when Installer adds Modules to the Module List	2		Yes			
MODULE CONFIG EDITED:	Occurs when the Installer alters a Module's hardware configuration settings	2		Yes			
ACCESS PART EDITED:	Occurs when Installer alters Access Partition Configuration	2		Yes			
NAMES EDITED:	Occurs when a User Edits the Name Pool entries	2		Yes			
SKEL CARDS EDITED:	Occurs when Installer alters Skeleton Card Configuration	2		Yes			
SKEL PINS EDITED:	Occurs when Installer alters Skeleton PIN Configuration	2		Yes			
BURG OPTS EDITED:	Occurs when Installer alters Burglary Options Settings	2		Yes			
DST OPTIONS EDITED:	Occurs when a User alters the Daylight Savings Time Settings.	2		Yes			
CARD RECOGNIZERS EDITED:	Occurs when Installer alters Card Recognizer Settings	2		Yes			
SCRIPT EDITED:	N/A in this Revision. Occurs when Script is altered	2		Yes			

Configuration Setting Changes (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to CS?	Defaulted to Dial to CS?	Contact ID Code
EV-ACT RLTN EDITED:	Occurs when a User alters an Event-Action Relationship	2		Yes			
HOLIDAYS EDITED:	Occurs when a User alters the Holiday List	2		Yes			
DAY TEMPLATE EDITED:	Occurs when a User alters a Day Template	2		Yes			
SCHEDULE EDITED:	Occurs when a User alters a Schedule	2		Yes			
ACCESS GROUP EDITED:	Occurs when User alters an Access Group Configuration	2		Yes			
SYSTEM PRESETS EDITED:	Occurs when the Installer alters the System Preset information	2		Yes			
ADMIN OPTIONS EDITED:	Occurs when a User alters the Administration Options	2		Yes			
SYS CONSOLE PARM EDITED:	The Installer has altered the System Console configuration settings.	2		Yes			
CONT-ID BASE PNTS EDITD:	This event occurs when the Installer modifies the Contact Id format Point Codes.	2		Yes			
EVENT PRI EDITED:	This event occurs when a user alters the event priority list.	2		Yes			
EVENT LOG CLEARED:	This event occurs when a user clears all event log contents.	2		Yes	Yes	Yes	E621 Event Log Cleared
READER GROUP EDITED:	Occurs when a User alters the Membership of a Reader Group	2		Yes			
RELAY GROUP EDITED:	Occurs when a User alters the Membership of a Relay Group	2		Yes			
TRIGGER GROUP EDITED:	Occurs when a User alters the Membership of a Trigger Group	2		Yes			

<b>Configuration Setting Changes (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to CS?</b>	<b>Defaulted to Dial to CS?</b>	<b>Contact ID Code</b>
ACCPT GROUP EDITED:	Occurs when a User alters the Membership of an Access Point Group	2		Yes			
ZONE GROUP EDITED:	Occurs when a User alters the Membership of a Zone Group	2		Yes			
CARD ADDED:	Occurs when a Cardholder is added	2		Yes			
CARD EDITED:	Occurs when a Cardholder's configuration data is altered	2		Yes			
CARD DELETED:	Occurs when a Cardholder is deleted from the system	2		Yes			

<b>Access Point Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
PROTECT ACCESS POINT:	Occurs when an Access Point is set to it's normal operation state. In Protect Mode, the Access Point will service entries and exits as determined by the Access Point's configuration.	1		Yes	Yes	Yes	R577 Access Point Protect
BYPASS ACCESS POINT:	Occurs when an Access Point has been set to Bypassed Mode. This Access Point no longer requires Card swipes or RTE Zone Faults to request Entry or Exits. The locking mechanism is disengaged, and the door can swing freely.	1		Yes	Yes	Yes	E577 Access Point Bypass

Access Point Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
EXIT ONLY ACCESS POINT:	Occurs when an Access Point is set to Exit-Only mode. The Access Point will only accept requests to exit through the Access Point either via an RTE Zone or an Exit Reader.	1		Yes	Yes	Yes	R577 Access Point Protect
TIMED BYP ACCPT START:	Occurs when an Access Point has been set to Timed Bypassed Mode. This Access Point no longer requires Card swipes or RTE Zone Faults to request Entry or Exits. The locking mechanism is disengaged, and the door can swing freely. The Access Point will automatically return to the Protected Mode at the expiration of the given time period.	1		Yes	Yes	Yes	E577 Access Point Bypass
TIMED BYP->PROT ACCPT:	Occurs when an Access Point is automatically set to it's normal operation state. In Protect Mode, the Access Point will service entries and exits as determined by the Access Point's configuration.	1		Yes	Yes	Yes	R577 Access Point Protect
LOCK ACCESS POINT:	Occurs when an Access Point is set to the Locked operational state. When Locked, the Access Point will not accept any entry or exit requests.	1		Yes	Yes	Yes	R577 Access Point Protect

<b>Access Point Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
SHUNT ACCPT DSM:	Occurs when an Access Point's Door Status Monitor Zone is Shunted. The Access Point will operate as though it did not have a Door Status Monitor Zone assigned and wired to it. This might have been done by a user if the DSM Zone is awaiting repair.	1		Yes	Yes	Yes	E433 Access Point DSM Shunt
UNSHUNT ACCPT DSM:	Occurs when an Access Point's Door Status Monitor Zone is Unshunted. The Access Point will once again operate using the Door Status Monitor Zone assigned and wired to it. This might have been done by a user if the DSM Zone returns to normal operation (ie. it was repaired).	1		Yes	Yes	Yes	R433 Access Point DSM Unshunt
SHUNT ACCPT RTE:	N/A in this revision. Occurs when an Access Point's Request to Exit Zone is Shunted. The Access Point will operate as though it did not have a RTE Zone assigned and wired to it. This might have been done by a user if the RTE Zone is awaiting repair.	1		Yes	Yes	Yes	E433 Access Point RTE Shunt
UNSHUNT ACCPT RTE:	N/A in this revision. Occurs when an Access Point's Request to Exit Zone is Unshunted. The Access Point will once again operate using the RTE Zone assigned and wired to it. This might have been done by a user if the RTE zone returns to normal operation (ie. it was repaired).	1		Yes	Yes	Yes	E433 Access Point RTE Unshunt

Access Point Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
ACCPT RESUME:	The Access Point was set to resume any scheduled operation.	1		Yes			
EXIT ONLY ACCPT GRP:	Occurs when an Access Point Group is set to Exit-Only	1		Yes			
PROTECT ACCPT GRP:	Occurs when an Access Point Group is set to Protect	1		Yes			
BYPASS ACCPT GRP:	Occurs when an Access Point Group is set to Bypassed	1		Yes			
LOCK ACCPT GRP:	Occurs when an Access Point Group is set to Locked	1		Yes			
ACCPT CLEAR PREC:	The precedence level of the Access Point was cleared to zero. Any initiator may now control this Access Point.	1		Yes			
ACCPT GRP CLEAR PREC:	The precedence level of all the Access Points in the indicated Access Point Group were cleared to zero. Any initiator may now control these Access Points.	1		Yes			
ACCPT GROUP RESUME:	The Access Points in the given Access Point Group were set to resume any scheduled operation.	1		Yes			
ACCPT NO ANTIPASSBACK:	Occurs when an Access Point is set to have no Anti-Passback restrictions.	1		Yes			
ACCPT SOFT ANTIPASSBACK:	Occurs when an Access Point is set to have Soft Anti-Passback restrictions. Cardholders who violate the Anti-Passback rules will generate a Soft Anti-Passback Violation Event, but will be granted Access.	1		Yes			

<b>Access Point Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCPT HARD ANTIPASSBACK:	Occurs when an Access Point is set to have Hard Anti-Passback restrictions. Cardholders who violate the Anti-Passback rules will be Denied Access.	1		Yes			

<b>Relay Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
RELAY ON:	Occurs when an Relay Output is turned ON, and the Relay is configured for "Controlled" operation. The Normally open contacts of the Form-C Relay will be connected, and the normally closed contacts of the Form-C Relay will be disconnected.	1	Yes	Yes			
RELAY OFF:	Occurs when an Relay Output is turned OFF, and the Relay is configured for "Controlled" operation. The Normally open contacts of the Form-C Relay will be disconnected, and the normally closed contacts of the Form-C Relay will be connected.	1	Yes	Yes			

Relay Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
RELAY CYCLE INITIATED:	Occurs when an Relay Output is turned ON, and the Relay is configured for "One-Shot" or "Repeating" operation. The contacts of the Output Relay will behave in a cyclic manner.	1	Yes	Yes			
RELAY CYCLE ENDED:	Occurs when an Relay Output is automatically turned OFF, after the execution of the specified number of repeat counts when the Relay is configured for "Repeating" operation. The Normally open contacts of the Form-C Relay will be disconnected, and the normally closed contacts of the Form-C Relay will be connected.	1	Yes	Yes			
RELAY CYCLE ABORTED:	Occurs when an Relay Output is turned OFF, and the Relay is configured for "One-Shot" or "Repeating" operation. The Normally open contacts of the Form-C Relay will be disconnected, and the normally closed contacts of the Form-C Relay will be connected.	1	Yes	Yes			
RELAY DISABLED:	This event occurs when an Output Relay is Disabled. The Output Relay will remain in it's current state (on or off) until Enabled. Relay On and Relay Off commands will no longer be responded to for this Output Relay.	1		Yes	Yes	Yes	E520 Relay Disable
RELAY ENABLED:	This event occurs when an Output Relay is Enabled. The Output Relay will return to a commandable state.	1		Yes	Yes	Yes	R520 Relay Enable



<b>Relay Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
RELAY GROUP DISABLED:	Occurs when a Relay Group is Disabled	1		Yes			
RELAY GROUP ENABLED:	Occurs when a Relay Group is Disabled	1		Yes			
RELAY RESUME:	The Output Relay was set to resume any scheduled operation.	1		Yes			
RELAY GROUP ON:	Occurs when a Relay Group is turned On	1		Yes			
RELAY GROUP OFF:	Occurs when a Relay Group is turned Off	1		Yes			
RELAY CLEAR PREC:	The precedence level of the Output Relay was cleared to zero. Any initiator may now control this Output Relay. Yes	1		Yes			
RELAY GROUP CLEAR PREC:	The precedence level of all the Output Relays in the indicated Relay Group were cleared to zero. Any initiator may now control these Output Relays.	1		Yes			
RELAY GROUP RESUME:	The Output Relays in the given Relay Group were set to resume any scheduled operation.	1		Yes			

<b>Trigger Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
TRIGGER ON:	Occurs when a Output Trigger is turned ON, and the Trigger is configured for "Controlled" operation. The open-collector Trigger Output will sink current.	1	Yes	Yes			

Trigger Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
TRIGGER OFF:	Occurs when a Output Trigger Output is turned OFF, and the Relay is configured for "Controlled" operation. The open-collector Trigger Output will go to a high-impedance state and cease to draw current.	1	Yes	Yes			
TRIGGER CYCLE INITIATED:	Occurs when an Output Trigger is turned ON, and the Trigger is configured for "One-Shot" or "Repeating" operation. The open collector Output Trigger will behave in a cyclic manner.	1	Yes	Yes			
TRIGGER CYCLE ENDED:	Occurs when an Output Trigger is automatically turned OFF, after the execution of the specified number of repeat counts when the Trigger is configured for "Repeating" operation. The open-collector Trigger Output will go to a high-impedance state and cease to draw current.	1	Yes	Yes			
TRIGGER CYCLE ABORTED:	Occurs when an Output Trigger is turned OFF, and the Trigger is configured for "One-Shot" or "Repeating" operation. The open-collector Trigger Output will go to a high-impedance state and cease to draw current.	1	Yes	Yes			

<b>Trigger Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
TRIGGER DISABLED:	This event occurs when an Output Trigger is Disabled. The Output Trigger will remain in it's current state (on or off) until Enabled. Trigger On and Trigger Off commands will no longer be responded to for this Output Trigger.	1		Yes	Yes	Yes	E520 Relay Disabled
TRIGGER ENABLED:	This event occurs when an Output Trigger is Enabled. The Output Trigger will return to a commandable state.	1		Yes	Yes	Yes	R520 Relay Enabled
TRIGGER GROUP DISABLED:	Occurs when a Trigger Group is Disabled	1		Yes			
TRIGGER GROUP ENABLED:	Occurs when a Trigger Group is Disabled	1		Yes			
TRIG RESUME:	The Output Trigger was set to resume any scheduled operation.	1		Yes			
TRIG GROUP ON:	Occurs when a Trigger Group is turned On	1		Yes			
TRIG GROUP OFF:	Occurs when a Relay Group is turned Off	1		Yes			
TRIG CLEAR PREC:	The precedence level of the Output Trigger was cleared to zero. Any initiator may now control this Trigger.	1		Yes			
TRIG GROUP CLEAR PREC:	The precedence level of all the Output Triggers in the indicated Trigger Group were cleared to zero. Any initiator may now control these Triggers.	1		Yes			
TRIG GROUP RESUME:	The Output Triggers in the given Trigger Group were set to resume any scheduled operation.	1		Yes			

<b>Reader Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
READER DISABLED:	This event occurs when an Uncommitted Reader is Disabled. The Reader will no longer process Card Swipes.	1		Yes	Yes	Yes	E501 Reader Disable
READER ENABLED:	This event occurs when an Uncommitted Reader is Enabled. The Reader will process Card Swipes.	1		Yes	Yes	Yes	R501 Reader Enable
READER GROUP DISABLED:	Occurs when a Reader Group is Disabled	1		Yes			
READER GROUP ENABLED:	Occurs when a Reader Group is Disabled	1		Yes			
READER RESUME:	The Uncommitted Reader was set to resume any scheduled operation.	1		Yes			
READER CLEAR PREC:	The precedence level of the Uncommitted Reader was cleared to zero. Any initiator may now control this Reader.	1		Yes			
READER GROUP CLEAR PREC:	The precedence level of all the Uncommitted Readers in the indicated Reader Group were cleared to zero. Any initiator may now control these Readers.	1		Yes			
READER GROUP RESUME:	The Uncommitted Readers in the given Reader Group were set to resume any scheduled operation.	1		Yes			
READER EVENT:	A card was swiped at an Uncommitted Reader.	1	Yes	Yes			
READER ACK:	A card was used at an Uncommitted Reader and the swipe was processed as accepted.	0	Yes				

<b>Reader Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
READER NACK:	A card was used at an Uncommitted Reader and the swipe was processed as denied.	0	Yes				
READER ID METH:	Occurs when an Uncommitted Reader's Identification Method is altered. For example, this occurs when the Id Method of a Reader is changed to Card followed by PIN	1		Yes			

<b>Zone Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
BYPASS ZONE:	Occurs when an Uncommitted Zone is Bypassed. This zone will no longer cause an alarm.	1		Yes	Yes	Yes	E570 Zone Bypass
PROTECT ZONE:	Occurs when an Uncommitted Zone is Bypassed. This zone will may cause an alarm if the Burglary System is armed appropriately for the zone's response type.	1		Yes	Yes	Yes	R570 Zone Bypass Restore
BYPASS ZONE GROUP:	Occurs when a Zone Group is Bypassed	1		Yes			
PROTECT ZONE GROUP:	Occurs when a Zone Group is Protected	1		Yes			
SHUNT ZONE:	Occurs when an Uncommitted Zone is Shunted. This zone's status will no longer be monitored by the system. The zone can no longer cause an alarm.	1		Yes	Yes	Yes	E576 Zone Shunt

<b>Zone Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
UNSHUNT ZONE:	Occurs when an Uncommitted Zone is Unshunted. The system will once again monitor the zone input. This zone will may cause an alarm if the Burglary System is armed appropriately for the zone's response type.	1		Yes	Yes	Yes	R576 Zone Unshunt
ZONE CLEAR PREC:	The precedence level of the Uncommitted Input Zone was cleared to zero. Any initiator may now control this Zone.	1		Yes			
ZONE GROUP CLEAR PREC:	The precedence level of all the Uncommitted Input Zones in the indicated Zone Group were cleared to zero. Any initiator may now control these Zones.	1		Yes			
ZONE GROUP RESUME:	The Uncommitted Input Zones in the given Zone Group were set to resume any scheduled operation.	1		Yes			
ZONE RESUME:	The Uncommitted Input Zone was set to resume any scheduled operation.	1		Yes			

<b>Other Control Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
PRECEDENCES CLEARED:	Precedences of all Access Points, Output Relays, Output Triggers, Uncommitted Zone Inputs and Uncommitted Readers were cleared to zero. Any initiator may now control these resources.	1		Yes			
SCRIPT DISABLED:	The indicated Script Function will no longer execute when invoked.	1		Yes			
SCRIPT ENABLED:	The indicated Script Function will execute when invoked.	1		Yes			
SCRIPT TIMER EXPIRED:	This event occurs when a programmatic script timer decrements to 0 seconds	1		Yes			
SCRIPT TIMER CLEARED:	This event occurs when a programmatic script timer is forcefully cleared to 0 seconds - generally to prevent and event/action this is programmed to happen on the script timer expiration from firing.	1		Yes			

Scheduling Related Events							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
SCHEDULES SYNCHRONIZED:	The Schedules were synchronized and re-evaluated. The Opening Action of all OPEN schedules was executed.	1		Yes			
DST START:	Daylight Savings Time was Started.	1		Yes			
DST END:	Daylight Savings Time was Ended.	1		Yes			

Access Control Related Events							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
THREAT LEVEL CHANGED:	Occurs when the operational Threat Level of the system is altered	5		Yes	Yes	Yes	E431 Threat Lvl Chg
EGRESS REQUEST:	A card was swiped at an Exit Reader of an Access Point.	1	Yes	Yes			
ACCESS REQUEST:	A card was swiped at an Entry Reader of an Access Point.	1	Yes	Yes			
DURESS ACCESS EVENT:	A duress PIN code was used at an Entry Reader of an Access Point. The cardholder was granted access.	4		Yes	Yes	Yes	E124 Duress Acc Grt
DURESS EGRESS EVENT:	A duress PIN code was used at an Exit Reader of an Access Point. The cardholder was granted egress.	4		Yes	Yes	Yes	E125 Duress Egr Grt
EXEC ACCESS GRANT:	A cardholder who's card was configured as having Executive Priviledges was granted access.	1		Yes	Yes	Yes	E422 Acc Grt



<b>Access Control Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCESS GRANT:	A cardholder was granted access.	1		Yes	Yes	Yes	E422 Acc Grt
EXEC EGRESS GRANT:	A cardholder who's card was configured as having Executive Priviledges was granted egress.	1		Yes	Yes	Yes	E425 Egr Grt
EGRESS GRANT:	A cardholder was granted egress.	1		Yes	Yes	Yes	E425 Egr Grt
PIN RETRY LOCKOUT:	A tamper condition has ocured indicateing that too many invalid PIN entries were attempted at an Access Point. The number of tries are configureable by the Installer, as is the number of seconds for which the Access Point will be ignored following the tamper condition.	1		Yes			
MANUAL ACCESS GRANT:	A user manually granted an Access cycle at an Access Point.	1		Yes			
MAN ACCESS GRANT W/TIME:	A user manually granted an Access cycle at an Access Point. Special timing parameters were used by this grant, such as unlock time, door open time, and pre-alarm timing.	1		Yes			
EGRESS DENIED:	A cardholder swiped invalidly at an Access Point's Entry Reader. See Access Denied event for reason list.	1		Yes	Yes	Yes	E425 Egress Denied



Access Control Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
ACCPT DOOR TIME:	After granting access or egress, an Access Point Door was held open longer than the allotted Door Open Time. The Access Point will not accept card swipes until the door is closed properly. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	2		Yes	Yes	Yes	E426 Door Prop Alarm
ACCPT DOOR TIME REST:	After granting access or egress, an Access Point Door that was held open longer than the allotted Door Open Time has been closed properly. The Access Point will now revert to normal operation. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	2		Yes	Yes	Yes	R426 Door Prop Alarm Restore
ACCPT DOOR OPEN ALARM:	An Access Point Door was forced open without proper access or egress being granted. The Access Point will not accept card swipes until the door is closed properly. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	3		Yes	Yes	Yes	E423 Door Force Alarm
ACCPT DOOR OPEN REST:	An Access Point Door was forced open without proper access or egress being granted has been closed. The Access Point will will now revert to normal operation. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	3		Yes	Yes	Yes	R423 Door Force Alarm Restore

<b>Access Control Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCPT ACC GRANT NO ENTR:	An Access Grant Event occurred, but no one opened the door to enter the protected area. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	1	Yes	Yes			
ACCPT EGR GRANT NO EGRS:	An Egress Grant Event occurred, but no one opened the door to exit the protected area. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	1	Yes	Yes			
ACCPT RTE GRANT NO EGRS:	A request to exit was performed, but no one opened the door to exit the protected area. This event can only occur if a Door Status Monitor Zone and a Request to Exit Zone is configured for the Access Point.	1	Yes	Yes			
ACCPT RTE GRANTED:	A request to exit was performed. This event can only occur if a Request to exit Zone is configured for the Access Point.	1	Yes	Yes			
ACCPT RTE RETRIGGERED:	A request to exit was performed while the door was still open. This event can only occur If a Request to Exit Zone and a Door Status Monitor Zone is configured for the Access Point.	1		Yes			

Access Control Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
ACCESS DENY OVR:	Access was granted due to a Deny Override condition. This generally means that the cardholder would have been denied, but since the Administration option of Deny Override was set, the cardholder was granted. The reason why the card was denied will also be displayed.	1		Yes	Yes	Yes	E422 Access Grant
EGRESS DENY OVR:	Egress was granted due to a Deny Override condition. This generally means that the cardholder would have been denied, but since the Administration option of Deny Override was set, the cardholder was granted. The reason why the card was denied will also be displayed.	1		Yes	Yes	Yes	E425 Egress Grant
ACC DENY OVR UNKN:	An unknown card was granted access due to a Deny Override condition. This generally means that the unknown card would have been denied, but since the Administration option of Deny Override was set, the card was granted.	1		Yes	Yes	Yes	E422 Access Grant
EGR DENY OVR UNKN:	An unknown card was granted egress due to a Deny Override condition. This generally means that the unknown card would have been denied, but since the Administration option of Deny Override was set, the card was granted.	1		Yes	Yes	Yes	E422 Egress Grant

<b>Access Control Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
CARDHLDR IN WRONG PARTN:	The Cardholder was denied, and the current location of the cardholder was checked and found that the cardholder has somehow traversed into an area in which they should not be. The cardholder was found to be in the wrong Access Partition.	1		Yes			
VISUAL VERIFICATION REQ:	A user was asked to visually verify a cardholder.	5		Yes			
ACCESS DENIED W/DR OPEN:	Access was denied to a cardholder, but the door was already open. This means that an invalid cardholder may have entered the premises.	3		Yes	Yes	Yes	E421 Access Denied
EGRESS DENIED W/DR OPEN:	Egress was denied to a cardholder, but the door was already open. This means that an invalid cardholder may have exited the premises.	3		Yes	Yes	Yes	E424 Egress Denied
ACCPT DOOR OPEN:	During Bypass Mode, an Access Point Door opened. This event will only occur if Door Status Monitor Zone is configured for the Access Point.	1		Yes			
ACCPT DOOR CLOSED:	During Bypass Mode, an Access Point Door closed. This event will only occur if Door Status Monitor Zone Is configured for the Access Point.	1		Yes			
ACCESS GRP NO EN/EX:	The indicated Access Group was configured to disregard any Entry/Exit requirements.	1		Yes			

Access Control Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
ACCESS GRP SOFT EN/EX:	The indicated Access Group was configured to abide by the Entry/Exit requirements. However, if a member of the Access Group violates the Entry/Exit rules, the cardholder may be granted access or egress, depending on the remaining access control constraints. However, a Soft Entry/Exit Violation event will be generated.	1		Yes			
ACCESS GRP HARD EN/EX:	The indicated Access Group was configured to abide by the Entry/Exit requirements. Depending on the remaining access control constraints, the cardholder may be denied access due to the violation.	1		Yes			
SOFT EN/EX VIOLATION:	A cardholder was granted access or egress but was detected as violating the Entry/Exit rules.	1		Yes			
SOFT ANTIPB VIOLATION:	A cardholder was granted access or egress, but was detected as violating the Anti-Passback rules. This event can only occur at an Access Point that was set to operate in Soft Anti-Passback Mode. Note that Hard Anti-Passback violations would have resulted in a denial of access or egress.	1		Yes			
CARD TRACE EVENT:	A card that was set to generate a Trace event was swiped at an Uncommitted Reader or at the Entry or Exit Reader of an Access Point.	4		Yes			

<b>Access Control Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCPT ENTRY ID METH:	Occurs when an Access Point's Entry Identification Method is altered. For example, this occurs when the Entry Id Method of an Access Point is changed to Card followed by PIN	1		Yes			
ACCPT EXIT ID METH:	Occurs when an Access Point's Exit Identification Method is altered. For example, this occurs when the Exit Id Method of an Access Point is changed to Card followed by PIN	1		Yes			
ACCPT NO VISUAL VER:	Occurs when an Access Point is set to have no Visual Verification of the Cardholder before granting access.	1		Yes			
ACCPT VISUAL VERIF:	Occurs when an Access Point is set to require Visual Verification of the Cardholder before granting access. The user terminal at which a User will be prompted to visually verify the Cardholder will be specified.	1		Yes			
ALL ENTRY/EXIT FORGIVEN:	Occurs when a User Forgives all the Entry/Exit status of all Cardholders. All Cardholders will be given "one free-pass".	1		Yes			
ENTRY/EXIT FRGVN FOR CH:	Occurs when a User Forgives the Entry/Exit status of a single Cardholder. The Cardholder will be given "one free-pass".	1		Yes			
ALL ANTIPB FORGIVEN:	Occurs when a User Forgives all the Anti-Passback status of all Cardholders. All Cardholders will be given "one free-pass".	1		Yes			

<b>Access Control Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ANTIPB FORGIVEN AT ACCTP:	Occurs when a User Forgives the Anti-Passback status of all Cardholders who have passed through a given Access Point. The Cardholders will be given "one free-pass".	1		Yes			
ANTIPB FORGIVEN FOR CH:	Occurs when a User Forgives the Anti-Passback status of a single Cardholder. The Cardholder will be given "one free-pass".	1		Yes			
ACCESS GROUP DISABLED:	Occurs when an Access Group is Disabled	1		Yes			
ACCESS GROUP ENABLED:	Occurs when an Access Group is Enabled	1		Yes			
UNRECOGNIZABLE CARD:	A card was swiped at a card reader that had an unrecognizable format.	1		Yes			
CARD EXP COUNTS BACK UP:	This event indicates that the Access Control System has permanently stored any access card expiration counts. This will occur once a day, as well as whenever the system is shut down or program mode is entered.	1		Yes			

<b>Remote Connection Related Messages</b>							
These events will only occur if the Access Control System is administered remotely using modem communications.							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
MODEM ERROR:	The Access Control System is experiencing trouble communicating with a modem.	2		Yes	Yes	Yes	E333 Module Comm Fail



<b>Remote Connection Related Messages (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
MODEM RESTORE:	The Access Control System has successfully communicated with a modem after experiencing a modem error.	2		Yes	Yes	Yes	R333 Module Comm Fail Rest
CAN NOT CONNECT:	The Access Control System could not reach its PC Host.	2		Yes	Yes	Yes	E354 Fail to Comm
BAD MODEM INIT STRING:	The Modem Initialization String has been configured improperly.	2		Yes			
BAD DIAL PREAMBLE STRING:	The Modem Dialing Preamble String has been configured improperly.	2		Yes			
BAD PHONE NUMBER:	The Modem Phone Book Phone Numbers have been configured improperly.	2		Yes			
BAD CONN COMPL STRNG:	The Modem Connection Completion String has been configured improperly.	2		Yes			
DIALOUT INITIATED:	The system has initiated an outgoing call to a host PC in order to upload event history. The reason for the call will be given.	2		Yes			
CALL IN ANSWERED:	The system has answered a call using its modem.	2		Yes			
REMOTE CNCT TERMTD-NORM:	A modem based remote connection was terminated normally.	2		Yes			
REMOTE CNCT TERMTD-NOCA:	A modem based remote connection was terminated due to a loss of modem carrier signal.	2		Yes			
REMOTE LOGIN TIMEOUT:	The allotted time for a PC User to log in for a remote modem based connection expired without a successful login. The system terminated the remote connection.	2		Yes			



DEFLT PHNEBK ENTRY USED:	After not being able to find the appropriate phone book entry, the Access System called the first phone number by default.	2		Yes			
--------------------------	--	---	--	-----	--	--	--

<b>Diagnostic and Test Mode Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCPT RTE ZNE TRB:	The Request to Exit Zone of an Access Point is experiencing a wiring trouble condition. This event can only occur if a Request to Exit Zone is configured for the Access Point.	2		Yes	Yes	Yes	E428 Access Point RTE Trouble
ACCPT RTE TRB REST:	The Request to Exit Zone of an Access Point is no longer experiencing a wiring trouble condition. This event can only occur if a Request to Exit Zone is configured for the Access Point.	2		Yes	Yes	Yes	R428 Access Point RTE Trouble Restore
ACCPT DSM ZNE TRB:	The Door Status Monitor Zone of an Access Point is experiencing a wiring trouble condition. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	2		Yes	Yes	Yes	E427 Access Point DSM Trouble
ACCPT DSM TRB REST:	The Door Status Monitor Zone of an Access Point is no longer experiencing a wiring trouble condition. This event can only occur if a Door Status Monitor Zone is configured for the Access Point.	2		Yes	Yes	Yes	R427 Access Point DSM Trouble Restore

<b>Diagnostic and Test Mode Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ACCPT RELAY SUPV FAIL:	The Door Control Relay of an Access Point that operates the door's locking mechanism has detected that the locking device's power has failed. This event can only occur if the Access Point's Door Control Relay was configured to monitor the voltage of the locking device.	2		Yes	Yes	Yes	E432 Access Point Relay Supervision Fail
ACCPT RLY SUPV REST:	The Door Control Relay of an Access Point that operates the door's locking mechanism has detected that the locking device's power has returned. This event can only occur if the Access Point's Door Control Relay was configured to monitor the voltage of the locking device.	2		Yes	Yes	Yes	R432 Access Point Relay Supervision Restore
RELAY SUPV FAIL:	The Output Relay has detected that its controlled device's power has failed. This event can only occur if the Output Relay was configured to monitor the voltage of the controlled device.	2		Yes	Yes	Yes	E320 Relay Supervision Fail
RELAY SUPV REST:	The Output Relay detected that the power has returned to its controlled device. This event can only occur if the Output Relay was configured to monitor the voltage of the controlled device.	2		Yes	Yes	Yes	R320 Relay Supervision Restore
COMM FAIL:	The Main Logic Board has experienced a communications failure with the indicated module.	2		Yes	Yes	Yes	E333 Comm Fail

Diagnostic and Test Mode Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
COMM FAIL RESTORE:	The Main Logic Board has experienced a return of communications with the indicated module.	2		Yes	Yes	Yes	R333 Comm Fail Restore
LOW BATTERY:	A module within the system is experiencing a Low Battery condition. This event will only occur at modules which have been programmed to monitor their battery condition.	2		Yes	Yes	Yes	E338 Module Low Battery
LOW BATT RESTORE:	A module within the system that was experiencing a Low Battery condition has detected that the battery has now been properly charged. This event will only occur at modules which have been programmed to monitor their battery condition.	2		Yes	Yes	Yes	R338 Module Low Battery Restore
AC PWR LOSS:	A module within the system is experiencing an AC Loss condition. This event will only occur at modules which have been programmed to monitor their AC Power condition.	2		Yes	Yes	Yes	E342 Module AC Loss
AC PWR RESTORE:	A module within the system that was experiencing an AC Loss Condition has detected that the AC line power has now been re-applied. This event will only occur at modules which have been programmed to monitor their AC Power condition.	2		Yes	Yes	Yes	R342 Module AC Restore

<b>Diagnostic and Test Mode Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
WALK TEST ZONE MISSED:	This event indicates that a Burglary Walk Test was performed, but the indicated Uncommitted Zone was not successfully tested.	2		Yes			
REQUEST MODULE STATUS:	This event appears when a User manually initiates a module status request when doing module test.	1		Yes			
MODULE STATUS:	This event contains the instantaneous status of the indicated module's inputs. The information presented by this event can be decoded by diagnostic software.	1		Yes			
ZONE GLASS RESET:	This event occurs when a User initiates a latching glass break reset function. This process will reset a fired latching glass break detector.	1		Yes			
MODULE EEROM CS ERROR:	This is a diagnostic event that indicates that a module has detected a problem with its internal configuration data.	2		Yes			
SYSTEM RESET:	Occurs when the system powers up or resets in response to a user request.	2		Yes	Yes	Yes	E305 System Reset
SYSTEM SHUTDOWN:	Occurs when the system is shutdown due to a user request or in response to a power loss.	5		Yes	Yes	Yes	E308 System Shutdown
WALK TEST START:	Burglary System Walk Test Started by a User	1		Yes	Yes	Yes	E607 Burg Walk Test Start

<b>Diagnostic and Test Mode Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
WALK TEST END:	Burglary System Walk Test Started by a User	1		Yes	Yes	Yes	R607 Burg Walk Test End
WALK TEST MISSED:	N/A in this revision. Walk Test Time Period expired without a Walk Test being performed	2		Yes			
SCRIPT ERROR:	This event occurs when an internal error is encountered while executing an Action Script. The type of error that occurred will be displayed.	1		Yes			
MANUAL SYS RESET:	This event indicates that the Access Control System was deliberately reset by a User	1		Yes	Yes	Yes	E311 Engineer Reset
NETWORK INPUT OVERFLOW:	This event indicates that network message traffic within the Access Control System was too heavy and that one or more network communications messages may have been missed.	1		Yes			
CARD DECK CORRUPT:	The cardholder database was found to contain an error. A user should execute a cardholder deck database defragmentation.	2		Yes			
DIALER TEST:	A periodic test report was sent to a monitoring central station.	2		Yes	Yes	Yes	E602 Periodic Dialer Test
COMM FAIL:	A monitoring central station could not be reached	2		Yes	Yes	Yes	E350 Centrl Station Comm Fail

<b>Diagnostic and Test Mode Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
MODULE CONF UPDATED:	A peripheral module was re-programmed to its configured state. This event will occur when the system powers up or exits the Installer's Programming Mode.	1		Yes			
MODULE RESET OCCURRED:	A module within the system experienced a reset condition.	1		Yes	Yes	Yes	E339 Module Reset
MODULE WDRST OCCURRED:	A module within the system experienced a reset condition.	1		Yes	Yes	Yes	E339 Module Reset
DCM RCM EXIT:	A Door Control Module has exited Reduced Capability Mode.	2		Yes			
EVENT LOG TEXT MESSAGE:	This event occurs when an Action Script places free-form text into the Event History Log. The text will be displayed.	1		Yes			

<b>Uncommitted Zone Related Events</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ZONE TROUBLE:	A wiring trouble condition has occurred at the indicated Uncommitted Zone.	2		Yes	Yes	Yes	E380 Zone Trouble
ZONE TRB REST:	A wiring trouble condition has cleared at the indicated Uncommitted Zone.	2		Yes	Yes	Yes	R380 Zone Trouble Restore

<b>Uncommitted Zone Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ZONE ALARM:	A Zone Alarm condition has occurred at the indicated Uncommitted Zone.	3		Yes	Yes	Yes	E140 Zone Alarm
ZONE ALM REST:	A Zone Alarm condition has restored at the indicated Uncommitted Zone.	3		Yes	Yes	Yes	R140 Zone Alarm Restore
ZONE FAULT:	An Uncommitted Zone has been set to an off-normal condition.	1	Yes	Yes			
ZONE RESTORE:	An Uncommitted Zone has returned to its normal condition.	1	Yes	Yes			
BURG SYS ARMED AWAY:	Occurs when the Burglary System of the Access Control panel is Armed Away	3		Yes	Yes	Yes	C401 Close Away
BURG SYS ARMED STAY:	Occurs when the Burglary System of the Access Control panel is Armed Stay	3		Yes	Yes	Yes	C441 Close Stay
BURG SYS DISARMED:	Occurs when the Burglary System of the Access Control panel is Disarmed	3		Yes	Yes	Yes	O401 Open
BURG SYS FRC ARMED AWAY:	The Burglary subsystem of the Access Control System was Armed Away, automatically bypassing any zones that were faulted.	3		Yes	Yes	Yes	C401 Close Away
BURG SYS FRC ARMED STAY:	The Burglary subsystem of the Access Control System was Armed Stay, automatically bypassing any zones that were faulted.	3		Yes	Yes	Yes	C441 Close Stay



<b>Uncommitted Zone Related Events (Con't)</b>							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ALARM SOUNDER ON:	The Relay Output that has been assigned for use as the Burglary Sounder was turned On. The Normally open contacts of the Form-C Relay will be connected, and the normally closed contacts of the Form-C Relay will be disconnected. This will occur in response to an Alarm condition.	1		Yes			
ALARM SOUNDER TIMEOUT:	The Alarm Sounder Relay Output that has been assigned for use as the Burglary Sounder was turned Off due to the expiration of its timeout. The Normally open contacts of the Form-C Relay will be disconnected, and the normally closed contacts of the Form-C Relay will be connected. This will occur after an Alarm condition if the Alarm is not manually acknowledged by a User performing a Disarm and Alarm Silencing operation.	1		Yes			
ALARM SNDR SILENCED:	This event occurs when a User performs a Disarm and Alarm Silence Operation. This signifies that a manual action has caused the Alarm Sounder to be silenced.	1		Yes			
OP/CL TRIG ON:	The Output Trigger that was assigned to function as the Open/Close Trigger was turned on. The open-collector Trigger Output will sink current. This signifies that the Burglary portion of the Access Control System has been Armed Away or Armed Stay.	1		Yes			

Uncommitted Zone Related Events (Con't)							
Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
OP/CL TRIG OFF:	The Output Trigger that was assigned to function as the Open/Close Trigger was turned off The open-collector Trigger Output will return to a high impedance state and cease to draw current. This signifies that the Burglary portion of the Access Control System has been Disarmed.	1		Yes			
BURG TRIG ACTIVATED:	The Output Trigger that was assigned to function as the Burglary Trigger was turned on. The open-collector Trigger Output will sink current. This signifies that the Burglary portion of the Access Control System has responded to an Alarm condition.	1		Yes			
BURG TRIG DEACTIVATED:	The Output Trigger that was assigned to function as the Burglary Trigger was turned off The open-collector Trigger Output will return to a high impedance state and cease to draw current. This signifies that the Burglary portion of the Access Control System has been Disarmed.	1		Yes			

<b>Vista Related Events</b>							
The following events will only occur is a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
ZONE FAULT TO VISTA:	This event indicates that a Zone fault was reported to a connected Vista Alarm Panel.	1		Yes			
ZONE REST TO VISTA:	This event indicates that a Zone restore was reported to a connected Vista Alarm Panel.	1		Yes			
ZONE TRBL TO VISTA:	This event indicates that a Zone trouble was reported to a connected Vista Alarm Panel.	1		Yes			
ACCPT FAULT TO VISTA:	This event indicates that an Access Point Door Status Monitor Zone fault was reported to a connected Vista Alarm Panel.	1		Yes			
ACCPT REST TO VISTA:	This event indicates that an Access Point Door Status Monitor Zone restore was reported to a connected Vista Alarm Panel.	1		Yes			
ACCPT TRBL TO VISTA:	This event indicates that an Access Point Door Status Monitor Zone trouble was reported to a connected Vista Alarm Panel.	1		Yes			
REQUEST VISTA STATUS:	This event indicates that the Access Control System has requested status information from a connected Vista Alarm Panel.	1		Yes			
VISTA BURG ALARM:	This event indicates that a burglary alarm condition has occurred in the given Vista Burglary Partition.	3		Yes			

### Vista Related Events (Con't)

The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.

Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
VISTA BURG ALARM REST:	This event indicates that a burglary alarm condition has restored (cleared) in the given Vista Burglary Partition.	3		Yes			
VISTA FIRE ALARM:	This event indicates that a fire alarm condition has occurred in the given Vista Partition.	3		Yes			
VISTA FIRE ALARM REST:	This event indicates that a fire alarm condition has restored (cleared) in the given Vista Partition.	3		Yes			
VISTA PANIC/ DURESS ALRM:	This event indicates that a panic or duress alarm condition has occurred in the given Vista Burglary Partition.	4		Yes			
VISTA PNC/DURAL REST:	This event indicates that a panic or duress alarm condition has restored (cleared) in the given Vista Burglary Partition.	4		Yes			
VISTA ARMED AWAY:	This event indicates that the given Vista Alarm Partition was Armed Away.	3		Yes			
VISTA ARMED STAY:	This event indicates that the given Vista Alarm Partition was Armed Stay.	3		Yes			
VISTA ARMED MAXIMUM:	This event indicates that the given Vista Alarm Partition was Armed Maximum.	3		Yes			
VISTA ARMED INSTANT:	This event indicates that the given Vista Alarm Partition was Armed Instant.	3		Yes			
VISTA DISARMED:	This event indicates that the given Vista Alarm Partition was Disarmed.	3		Yes			

<b>Vista Related Events (Con't)</b>							
The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
VISTA LOW BATTERY:	This event indicates that the Vista Alarm Panel connected to the Access Control System is experiencing a Low Battery condition.	3		Yes			
VISTA LOW BATT REST:	This event indicates that the Vista Alarm Panel's Low Battery condition has restored and that its battery is charged.	3		Yes			
VISTA AC PWR LOSS:	This event indicates that the Vista Alarm Panel connected to the Access Control System has lost its AC line voltage.	3		Yes			
VISTA AC PWR RESTORE:	This event indicates that the Vista Alarm Panel's AC line voltage has been turned back on.	3		Yes			
VISTA DLR COMM FAIL:	This event indicates that the Vista Alarm Panel's central station communicator (dialer) has not been able to reach the central station.	2		Yes			
VISTA DLR COMM REST:	This event indicates that the Vista Alarm Panel's central station communicator (dialer) has been able to reach the central station after a period of failure.	2		Yes			
VISTA CMD TO UNKN ACCT:	This event indicates that the Vista Alarm Panel has attempted to control an Access Point that is invalid. This event may occur if the Vista Panel's User Code or keypad programming that maps to the Access Point is invalid.	2		Yes			

### Vista Related Events (Con't)

The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.

Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
ACCESS REQ FR UNKN VUSR:	This event indicates that the Vista Alarm Panel has requested access using a Vista User number that was unknown to the Access Control System. This can occur if the cardholder database in the Access Control System does not contain an entry indicating this Vista User Number.	2		Yes			
EGRESS REQ FR UNKN VUSR:	This event indicates that the Vista Alarm Panel has requested egress using a Vista User number that was unknown to the Access Control System. This can occur if the cardholder database in the Access Control System does not contain an entry indicating this Vista User Number.	2		Yes			
VISTA CONNECTION FAIL:	This event indicates that the Access Control System cannot communicate with its Vista Alarm Panel.	2		Yes			
VISTA CONNECTION REST:	This event indicates that the Access Control System can once again communicate with its Vista Alarm Panel after a period of communication failure.	2		Yes			
BYP VISTA ZONE LIST:	This event occurs when the Access Control System instructs the Vista Alarm Panel to bypass a Vista Panel Zone List.	1		Yes			

<b>Vista Related Events (Con't)</b>							
The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
PROTECT VISTA ZONE LIST:	This event occurs when the Access Control System instructs the Vista Alarm Panel to protect a Vista Panel Zone List.	1		Yes			
VISTA PART OPEN ENABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to enable openings (disarm operations) within the indicated Vista Burglary Partition.	1		Yes			
VISTA PART OPEN DISABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to disable openings (disarm operations) within the indicated Vista Burglary Partition.	1		Yes			
VISTA PART CLOSE ENABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to enable closings (arming operations) within the indicated Vista Burglary Partition.	1		Yes			
VISTA PART CLOSE DISABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to disable closings (arming operations) within the indicated Vista Burglary Partition.	1		Yes			
VISTA ACCESS GRP ENABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to enable a Vista Access Group.	1		Yes			

### Vista Related Events (Con't)

The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.

Event	Cause	Default Priority	Priority Editable	Logged	Can be Dialed to Central Station	Defaulted to Dial to Central Sta	Contact ID Code
VISTA ACCESS GRP DISABLE:	This event occurs when the Access Control System instructs the Vista Alarm Panel to disable a Vista Access Group.	1		Yes			
VISTA RELAY ON:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to turn on one of the Vista's Output Relays.	1		Yes			
VISTA RELAY OFF:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to turn on one of the Vista's Output Relays.	1		Yes			
VISTA RELAY PULSE:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relays.	1		Yes			
VISTA RELAY PULSE XXMIN:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relays for the duration specified by the XX minute timer as specified by the Vista Panel's programming options.	1		Yes			
VISTA RELAY PULSE YYSEC:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relays for the duration specified by the YY seconds timer as specified by the Vista Panel's programming options.	1		Yes			



<b>Vista Related Events (Con't)</b>							
The following events will only occur if a Vista Alarm Panel has been connected to the Access Control System through a VGM Module.							
<b>Event</b>	<b>Cause</b>	<b>Default Priority</b>	<b>Priority Editable</b>	<b>Logged</b>	<b>Can be Dialed to Central Station</b>	<b>Defaulted to Dial to Central Sta</b>	<b>Contact ID Code</b>
VISTA RELAY GRP ON:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to turn on one of the Vista's Output Relay Groups.	1		Yes			
VISTA RELAY GRP OFF:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to turn on one of the Vista's Output Relay Groups.	1		Yes			
VISTA RELAY GRP PULSE:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relay Groups.	1		Yes			
VISTA RLY GRP PULSE XXM:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relay Groups for the duration specified by the XX minute timer as specified by the Vista Panel's programming options.	1		Yes			
VISTA RLY GRP PULSE YYS:	This event indicates that the Access Control System has instructed the Vista Alarm Panel to pulse one of the Vista's Output Relay Groups for the duration specified by the YY seconds timer as specified by the Vista Panel's programming options.	1		Yes			



## Glossary

# G

## *Access Control Glossary*

### A

**Access Card** - A card, generally the size and shape of a credit card, containing encoded data. The data can be encoded in a variety of ways, sometimes including more than one encodation technology. (See Magnetic Stripe, Wiegand, Proximity.)

**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 that share common access privileges, in regards to 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 Partition/Access Area** - A completely enclosed space that is controlled for entry and egress. Generally, when a person passes into the area, PassPoint will note that the person is in the specified area. In this way, the system can keep track

of where people are within a facility. Note, however, that both entry to and egress from the area must be logged by the PassPoint system in order for this feature to work. That is, if the entry to an area is controlled by PassPoint but egress is not controlled by PassPoint, the system will not be notified when a person leaves the area. This will lead to incorrect occupancy reading of the protected areas.

**Access Point** - A collection of card readers, zones, triggers, and 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 which 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.

**Anti-Passback (APB)** - An Access Control function whereby a cardholder is prevented from “passing back” his card to another person to gain entry into the same area twice, without leaving. A parking garage would be a good example of such a situation. A boss may try to pass his card back to his secretary, so that they may both park in the executive parking lot. Facilities are typically fitted with both Entry and Exit readers when Anti-Passback is implemented. A cardholder must alternate usage between entry and exit readers. If the cardholder attempts to pass through an entry reader twice consecutively, the cardholder will generate an Anti-Passback violation. In addition, based on the configuration of the Access Control System, he may be denied access as a result of that violation. In ADEMCO’s implementation, it simply means attempting to use the same Access Point in the same direction within a specified period of time (without using that Access Point in the opposite direction).

**Archive** - A file stored on your system's PC that holds previously uploaded events. Archives allow you to keep and organize all of the events recorded by your system.

**Arm Away** - This is a function of the burglary sub-system of the PassPoint system. Arming the system enables zones to cause a burglary alarm. Arming the burglary sub-system in the Away mode implies that you will be away from the premises and enables Interior and Perimeter zone types so that they will cause an alarm when faulted.

**Arm Stay** - This is a function of the burglary sub-system of the PassPoint system. Arming the system enables zones to cause a burglary alarm. Arming the burglary sub-system in the Stay mode implies that you are staying on the premises and enables only the Perimeter and 24 Hour zones types.

**B**

**Biometrics** - Readers that identify human attributes such as fingerprint, hand geometry, voice recognition, or retinal scans.

**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".

**Bypass (Zone)** - When an alarm zone is placed in Bypass mode, it no longer generates alerts to the user when the zone changes state. You may want to Bypass an internal zone (such as a corridor) during the day, when you would expect activity, but no security violations are actually occurring.

**C**

**Card Reader** - A device used by Cardholders to identify themselves to the PassPoint 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

In some cases, the device used for identification may be a keypad rather than a card reader. Instead of presenting a card to the keypad, the Cardholder must enter their assigned Personal Identification Number (PIN code) in order to identify his/herself. In situations where higher security is required, the entry reader may be a combination unit which acts as both a keypad and a card reader.

**Cardholder** - An occupant of a premises who has been issued an access card or access code (or PIN, Personal Identification Number) which 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.

**CPM (Computer Port Module)** - The CPM acts as an enrollment station. The enrollment station cannot be committed to an Access Point.

**D**

**Day Template** - The part of a time schedule that is used to specify time intervals during the day that an action can occur. Day templates contain time "windows" that define start and stop times for actions. For example, A Day Template could contain the following time intervals or "windows": 07:00-

08:30, 12:00-13:00, 17:00-17:30. This Day Template could then be assigned to Monday through Friday of a schedule, and the schedule could then be assigned to a scheduled action upon window opening or closing. That action could be to bypass an Access Point during normal workdays. (See also: Schedules)

**DCM (Door Control Module)** - The DCM provides all the inputs and outputs required to manage one or two Access Points (i.e. doors). This may also be a single Access Point where Anti-Passback is implemented.

**Deny Override** - This function allows all cards to be granted access. When a system is initially installed, this feature can be enabled to allow all people to access all doors. The event history can then be reviewed and the configuration fine-tuned. After a week or so of careful monitoring, the feature can be disabled, and standard control can be enforced.

**Disarm** - This is a function of the burglary sub-system of the PassPoint system. Disarming the system disables zones from causing a burglary alarm.

Disarming the burglary sub-system in the Away mode disables Interior, Perimeter, and 24 Hour zone types so that they will not cause an alarm when faulted.

Disarming the burglary sub-system in the Stay mode disables only the Perimeter and 24 Hour zone types.

**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. You can have doors that have only a single card reader, or you

can have card reader/keypad combination units requiring an occupant to enter a PIN code after swiping his/her card. 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 which 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 a door is permitted to remain open after the door is unlocked, before an alarm is generated by the access control system.

**Door Strike** - An electromechanical locking device typically installed in a door frame 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 will reflect the state of the door (open or closed) and also allow the PassPoint to determine if the door has been forced open, or held open too long.

**Duress** - A condition whereby a cardholder may be confronted by an intruder in an effort to gain access to a secure area. The cardholder can “secretly” signal security that he is entering the secure area under “duress” through the implementation of a duress feature.



**E**

**Enrollment Reader** - A card reader (connected to a CPM) which can be used to enroll cards into the Access Control System.

**Entry/Exit Control** - A means of controlling and monitoring the flow of Cardholders through a building. It is used in conjunction with Access Groups to either allow or deny group members access to specific areas, based on their directional usage of Access Points.

**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 PassPoint 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 will be a card reader at which a Cardholder must present their ID card. However, the device may be a keypad at which the individual must enter their assigned Personal Identification Number (PIN code) in order to identify his/herself. In some cases, where higher security is required, the entry reader may be a combination unit which acts as both a keypad and a card reader.

**EOLR Supervision (End Of Line Resistor Supervision)** - A mode which 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 Relationship** - 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.

**Event Browser** - The PassPoint tool for viewing uploaded events. The Event Browser organizes all of the uploaded events by date and displays them on screen.

**Event Log (or History Log)** - A list of events which indicate the actions performed by and within the PassPoint system. Each event log entry contains the time, date, and any other attributes that specifically define the event.

**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 will only accept exit requests. Any entry reader will be ignored.

**Exit Reader** - An exit reader is an input device that is installed on the exit side of an Access Point door. At this device, an individual is required to identify his/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**

**Facility Code** - An encoded value (within the access card) which can be used to identify the facility or site that issued a specific group of cards. This information can be used in a reduced security environment whereby the specific card number is ignored, but anyone from that “facility” can gain access.

**Fail Safe** - A locking device which will automatically unlock in the event of power loss.

**Fail Secure** - A locking device which will automatically lock in the event of power loss.

**Force Arm Away** - Arms the burglary system in the away mode. Any faulted zones will be automatically bypassed.

**Force Arm Stay** - Arms the burglary system in the stay mode. Any faulted zones will be automatically bypassed.

**Forgive (Entry/Exit, Anti-Passback)** - Because Entry/Exit and Anti-Passback violations can result in access and egress denials, Cardholders can be “stuck” in the place where the violation is detected if their card swipes are denied. These functions permit the administrator to “forgive” Anti-Passback and Entry/Exit violations for a Cardholder and/or an Access Point. When these functions are used, the system's Anti-Passback and/or Entry/Exit mechanisms and records are re-synchronized so that Cardholders can continue through the premises.

**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**

**Hard Anti-Passback** - If a cardholder is in violation of Anti-Passback rules, he will not be granted access.

**Hard Entry/Exit** - If a cardholder is in violation of Entry/Exit rules, he will not be granted access.

**Holiday** - A component of time schedules that define 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 key strokes. The keypad will generally resemble a telephone keypad with respect to the relative positions and key name assignments.

**L** **Locked (Access Point)** - A mode which latches the door of the Access Point. The Access Point's readers will be disabled for access control functions. The Access Point will not allow any accesses or egresses in the Locked mode.

**M** **Magnetic Stripe** - The black or brown stripe typically found on the back of a credit card or access card. The stripe is encoded similarly to a cassette tape. That is, magnetic domains are impressed upon the material so that it can be read by a reader at a later time.

**Mag Lock (Magnetic Lock)** - A large coil of wire mounted to a door frame, which when current is passed through the coil, creates a strong magnetic field. A large metal plate is also secured to the door, and will be held tightly against the coil of wire, due to the presence of 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.

**MLB (Main Logic Board)** - The MLB is the main controller of the Access Control System. It contains the card database, the event log, and system configuration information. It also keeps track of the system status. The MLB receives its power from the Access Control power supply, and communicates with the Door Control Module (described above) to determine if access should be granted to a particular Access Point. It can also coordinate the activities of other system modules, such as the QRM or ZIM.

**Modem** - A device that converts digital information into analog information so it can be transmitted over telephone lines, and converts the received analog data back to digital data at the other end by another modem.

**N** **Name Pool** - A collection of names, assigned by a user, that can be applied to system objects (i.e. relays, readers, etc.) The name pool can contain a maximum of sixty names, each up to fifteen characters in length. This can also be known as “Custom Alpha Descriptors”.

**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).

**P** **PIN (Personal Identification Number)** - A number assigned to an individual that, when entered in to a keypad, will allow the Access Control System to grant access into a secure area. PINs can also be combined with encoded cards and biometric devices to ensure higher levels of security.

**PIN Retry Lockout** - A feature that disables the keypad of an entry reader for a specified amount of time after a specified number of improper PIN entries. PIN retry lockout protects the premises from intruders who tamper with a keypad controlled Access Point. It slows down the process of trying all possible code combinations. The system records an event when PIN Retry Lockout is initiated at an Access Point.

**PIR (Passive Infra Red)** - 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.

**Power supply (Access Control)** - The Access Control power supply provides all the power needed by the MLB and DCM. It is connected to the AC line voltage via an 18VAC, 50VA Basler-type plug-in power transformer. The power supply provides a battery backup/charger connection and supports a 7-AmpHour battery. In addition, it has the capability to monitor and test the AC power input and battery condition. The results of which are provided to the modules, and ultimately to the MLB.

**Pre-Alarm Trigger Time (P-A 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 will be energized.

For example, if the door is set to be allowed to remain open for 30 seconds, an appropriate pre-alarm time would be 10 seconds. After the door has been unlatched for 20 seconds, the system would then give 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 will occur. The pre-alarm device will remain energized (depending upon its mode) until the door is closed, clearing the Door Open Timeout Alarm.

**Precedence Level** - A type of authority level that tells the system when certain system resources can be controlled. Simply put, precedence levels determine whether or not an operation should take place over the authority of any other previously initiated action.

**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.

**Q** **QRM (Quad Relay Module)** - A module that can be placed on the Access Control network to provide four additional Form C, supervised outputs, in addition to four Trigger outputs.

**R** **RCM (Reduced Capability Mode)** - In the unlikely event of a DCM (Door Control Module) becoming “disconnected” from the rest of the PassPoint system, the DCM can be told how to act while it is out of contact with the MLB (Main Logic Board). When it is “out of contact,” the DCM is placed in Reduced Capability Mode (RCM).

**Reader** - A device that a Cardholder presents his access card to, that will read the card’s encoded data and transmit it to an

access control panel. The panel will then make a decision as to what action to take as a result of that card read (energize a relay, etc.).

**Relay Supervision** - The common pole of the Form C relay will be monitored for the presence of voltage. An alert will be generated if the voltage is not sensed. This might be used to sense if an external power supply (used for lock power) has failed.

**RTE (Request To Exit)** - A condition generated by a device (push-button, crash bar, PIR, switch floor mat, etc.) that indicates to PassPoint that someone is leaving the protected area. No card is required, and 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.

**Shunt (Access Point)** - This function disables the DSM zone on the Access Point. The Access Point will then operate as though it does not have a DSM zone installed. This function is useful in instances of hardware failure, when a bad door contact might hinder the operation of the Access Point. The Access Point can be operated in the shunted state until it is repaired.

**Shunt (Zone)** - Shunting a zone serves almost the same purpose as the Bypass Zone function except for one exception.



While the Bypass Zone function causes detected changes in zone status to occur without generating any alarms, Shunting a zone causes the zone to go unmonitored. This can be beneficial when there is a malfunctioning zone on a peripheral module. The peripheral module may be flooding the communications network with zone status change messages. Shunting the zone tells the appropriate peripheral module to ignore the applicable zone and stop sending status change messages. The zone can then be kept Shunted until it is repaired.

**Skeleton Codes (or Skeleton Cards)** - Skeleton codes are used to unlock Access Points during Reduced Capability Mode (RCM) operation. They are only used when the communication link between the MLB and its DCM has been interrupted. Under these conditions, the DCM uses these skeleton codes as a very small card database. When the communication link is restored and the system quits RCM mode, the skeleton code database is no longer utilized.

**Soft Anti-Passback** - If a cardholder is in violation of Anti-Passback rules, he will be granted access, but a record of the violation will be stored in the event history.

**Soft Entry/Exit** - If a cardholder is in violation of Entry/Exit rules, he will be granted access, but a record of the violation will be stored in the event history.

**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**

**Threat Level** - A global condition that can be set by system users to qualify a state of emergency. There are six threat levels, TL0 through TL5. TL5 is the highest threat level.

Threat Levels can also be set for individual actions, indicating the global Threat Level at which the action will be allowed to take place. If the global Threat Level goes beyond the setting for the action, the action will not be allowed to occur.

**Transaction** - An event that occurred within the access control system which generates a record in the stored database.

**Transient Suppression** - A process by which short term, high energy bursts can be limited to safe levels by the use of specialized electronic components. The purpose of this might be to protect sensitive electronic equipment connected over communications lines of considerable length.

**Trigger Outputs** - Trigger Outputs are 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 trouble condition generally indicates a problematic line (cable or connection) for a supervised zone.

**U**

**User (system)** - A person that interacts with the system through the system interface. Users can control readers, set time schedules, enroll ID cards, etc. There are four levels of users: Installer, Masters, Managers, Operators.

**User Code** - The identification code used by a user to gain access to the system. User codes are entered through the system interface.

**V** **VGM (Vista Gateway Module)** - The PassPoint component that provides an interface between the Ademco Vista Panel and the Ademco Access Control System. When Vista control is not used, the VGM acts as the dialer for the PassPoint system.

**Visual Verification** - An optional mode that requires the system to defer to an operator to visually verify the identity of all Cardholders after a Cardholder's card/PIN has already been verified by the system.

**W** **Watchdog Timer** - An internal circuit within the system that will reset the control electronics in the unlikely event that it becomes locked in an endless loop of some kind. This will allow the system to continue to operate even though there would have ordinarily been a problem that would have caused the system to 'lock up' or freeze.

**Wiegand** - A card reader technology relying on a series of wires imbedded in a vinyl card. The Wiegand card is passed through a Wiegand reader to communicate a distinguishing pattern of ones and zeroes to the access control system to identify a particular card holder. (What you have)

**Windows (Time)** - A time interval during a the day when actions are allowed to occur. Up to eight of these time windows can be contained within one Day Template.

**X** **XX Minutes Timer** - A timer that is programmed on the Vista Alarm Panel that expires after a preset number of minutes. Generally, a Vista Output Relay may be configured to operate

for the duration of the timer. This timer can be programmed at location 1\*74 on the Vista Panel.

**Y**

**YY Seconds Timer** - A timer that is programmed on the Vista Alarm Panel that expires after a preset number of seconds. Generally, a Vista Output Relay may be configured to operate for the duration of the timer. This timer can be programmed at location 1\*75 on the Vista Panel.

**Z**

**ZIM (Zone Input Module)** - A module that can be placed on the Access Control network to provide eight additional zone inputs, which can be configured as supervised or unsupervised.

**Zone** - An area or object being protected by an electronic circuit.