



# PASSPOINT PLUS

Installation and Setup Guide

**ADEMCO**  
GROUP  
INTEGRATED SYSTEMS

**NORTHERN**  
COMPUTERS, INC.



# PassPoint *Plus*

Release 2.00

---

## INSTALLATION and SETUP GUIDE

---

*For Access Control Kits*



K4879 03/00

### **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. 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 shown above.**

**Important:** This Software is security related. Access should be limited to authorized individuals.

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, non exclusive 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. License 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 the limitation on liability contained herein and that such provisions are fair and not unconscionable.

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 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.

DISCLAIMER OF WARRANTIES. ADEMCO does not warrant that the Licensed Programs will meet your requirements, that operation of the Licensed Programs will be uninterrupted or error-free, or that all Licensed Programs' errors will be corrected. The entire risk as to the quality and performance of the Licensed Programs is with you. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY ADEMCO, ITS EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENTS SHALL INCREASE THE SCOPE OF THE ABOVE WARRANTIES OR CREATE ANY NEW WARRANTIES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE LICENSED PROGRAMS. This warranty gives you specific legal rights. You may 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 or other media 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 that 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 Agreement 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, New York 11791.

9. LIMITATION OF LIABILITY. REGARDLESS OF WHETHER ANY REMEDY SET FORTH IN THIS AGREEMENT FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL ADEMCO OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE LICENSED PROGRAMS OR ANY DATA SUPPLIED THEREWITH EVEN IF ADEMCO OR ANYONE ELSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. THIS PROVISION IS INCLUDED FOR THE BENEFIT OF ADEMCO AND ITS LOCAL REPRESENTATIVES, AND IS ENFORCEABLE BY EACH OF THEM.

SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL THE LIABILITY OF THE LICENSED PROGRAMS' PROVIDERS OR OF ADEMCO EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT.

10. REGISTRATION. In order to qualify to receive notification of ADEMCO updates to the Licensed Programs, Licensee must complete and return a 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.

11. 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.

12. GENERAL. This agreement is the complete and exclusive statement of the understanding of the parties hereto 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, 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 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 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 expensed incurred including attorneys' fees in enforcing its right under this agreement.

# Table of Contents

## Section One – Setting Up PassPoint

---

<b>Introduction to Setup.....</b>	<b>1-1</b>
Understanding PassPoint Kits.....	1-2
System Hierarchy.....	1-3
What's In Section One? .....	1-5
About Your PassPoint Access Starter Kit.....	1-6
Installation and Setup Map .....	1-10
Where do you go from here? .....	1-11
 <b>Preparing for Your Installation .....</b>	 <b>2-1</b>
How Should You Prepare for Your Installation?.....	2-3
Ask Yourself Some Basic Questions.....	2-3
Question 1 - Where will my access points be? .....	2-4
Question 2 - What level of security should I have for my access points?.....	2-4
Question 3 - What type of door control hardware should I use?.....	2-4
Question 4 - Where will my system computer be located? .....	2-5
Use a Floor Plan .....	2-5
Selecting Your Access Points .....	2-8
Example 1 - Basic entry control .....	2-9
Example 2 - Entry control with Door Status Monitoring .....	2-10
Example 3 - Entry control with Door Status Monitoring and Request-to-Exit.....	2-11
Example 4 - Entry and exit control with Door Status Monitoring .....	2-12
Door Control Module configuration.....	2-13
Types of Card Readers.....	2-15
Where do you go from here? .....	2-17

<b>System Installation .....</b>	<b>3-1</b>
Summary of Installation Steps .....	3-3
Step 1 - Mount the System Panel .....	3-4
Step 2 - Connect the System Modules .....	3-5
Step 3 - Mount and Connect Card Readers.....	3-7
Mounting card readers .....	3-8
Connecting card readers .....	3-8
Step 4 - Mount and Connect Door Strikes and Magnetic Locks .....	3-10
Mounting door strikes and magnetic locks.....	3-11
Connecting door strikes and magnetic locks .....	3-11
Step 5 - Connect the Computer Cable.....	3-13
Hardwire Connection.....	3-13
Remote Terminal Connection.....	3-15
Step 6 - Mount and Connect the Keypad and Power Up the System .....	3-18
Step 7 - Connect the Optional 7 Ampere-Hour Battery.....	3-20
Where do you go from here? .....	3-21
<b>Software Setup.....</b>	<b>4-1</b>
What Is PassPoint Plus?.....	4-4
System Requirements .....	4-5
Step 1 - Install PassPoint Plus.....	4-7
Step 2 - Start PassPoint Plus .....	4-8
Step 3 - Create a New Account.....	4-9
The PassPoint Plus Environment.....	4-12
Major screen components .....	4-13
<b>System Configuration .....</b>	<b>5-1</b>
Step 1 - Run the Setup Wizard.....	5-4
Step 2 - Establish Communications .....	5-7
Step 3 - Auto Enroll Modules .....	5-9
Enrolling a Single Module.....	5-10
Enrolling Multiple Modules .....	5-11
Step 4 - Download the Database.....	5-13



<b>Managing Cards and the Cardholder Database.....</b>	<b>6-1</b>
About the Cardholder Database .....	6-2
Using the Card Wizard.....	6-4
Adding a single card .....	6-5
Adding a batch of cards .....	6-9
Adding Cards Manually .....	6-9
Using the Action tab .....	6-14
Using the Personal tab .....	6-16
Using the Employment tab .....	6-17
Using the Custom tab .....	6-18
Using the Summary tab .....	6-20
Using the Events tab .....	6-23
Bulk Editing Cards.....	6-24
Bulk editing cardholder access group assignments .....	6-27
Bulk editing cardholder executive privileges/trace .....	6-28
Bulk editing cardholder disabled/expiration data .....	6-29
Bulk editing cardholder custom fields.....	6-32
The Card Monitor .....	6-33
Creating the Card Monitor Tool .....	6-34
Using the Card Monitor.....	6-35
 <b>Setting System-Wide Options.....</b>	 <b>7-1</b>
PassPoint System-Wide Options .....	7-2
System presets (Presets tab) .....	7-3
Reader preset attributes .....	7-4
Access Point preset attributes .....	7-5
Card technology options (Card Tech tab).....	7-6
Card recognizer information.....	7-6
Card lengths.....	7-7
ABA MagStripe Configuration screen .....	7-8
ABA MagStripe configuration sample .....	7-14
Skeleton codes (Skeletons tab) .....	7-16
Creating and assigning skeleton card codes .....	7-19
Skeleton PIN codes.....	7-28
Burglary system options (Burg System tab).....	7-28

Burg configuration.....	7-29
System console .....	7-31
Console annunciations.....	7-31
Access point beeps and video (Acpt Beep/Video tab) .....	7-32
Dialer reporting options (Dialer Reports tab).....	7-33
Modem options (Modem tab) .....	7-33
Session properties .....	7-34
Phone book .....	7-35
Outgoing call initiators .....	7-35
Network ID options (Network/ID tab) .....	7-36
Network .....	7-37
Identification.....	7-37
Priority options (Priorities tab).....	7-38
Changing an Event's Priority .....	7-39
Changing an Event's Attributes.....	7-40
Defining Event Paging.....	7-42
Defining Event E-mailing.....	7-45
Creating Event Instructions .....	7-48
<b>Resource Lists.....</b>	<b>8-1</b>
Defining Resource Lists.....	8-2
Access Points tab.....	8-3
Readers tab .....	8-5
Relays tab .....	8-7
Triggers tab.....	8-8
Zones tab.....	8-10
Using Resource Lists .....	8-11

---

## **Section Two – Expanding PassPoint**

---

<b>Adding a Door Expansion Kit.....</b>	<b>9-1</b>
Understanding Your Door Expansion Kit.....	9-2

Installing the DEK .....	9-3
Step 1 - Mount the DEK panel .....	9-3
Step 2 - Connect the DCM .....	9-5
Step 3 - Activate the system .....	9-7
Step 4 - Add and set up the DCM.....	9-8
Step 5 - Auto enroll the DCM .....	9-14
Step 6 - Download the database .....	9-19
Configuring the DCM.....	9-20
DCM System tab .....	9-22
Access Point A/B tabs .....	9-22
Readers tab .....	9-35
Relay tab.....	9-36
Triggers tab.....	9-38
Zone tabs.....	9-40
Skeleton RCM tab .....	9-43
 <b>Adding a Card Enrollment Kit.....</b>	<b>10-1</b>
Understanding Your Card Enrollment Kit.....	10-2
Installing the CEK .....	10-3
Step 1 - Choose a location for the CEK.....	10-3
Step 2 - Connect the CEK to the system .....	10-3
Step 3 - Connect the power transformer and activate the system.....	10-4
Step 4 - Add and set up the CEK.....	10-5
Step 5 - Auto enroll the CPM.....	10-7
Step 6 - Configure the reader.....	10-12
Reader tab .....	10-13
User Terminal tab .....	10-15
Step 7 - Download the database .....	10-15
 <b>Adding a VISTA Gateway Module.....</b>	<b>11-1</b>
Understanding Your VISTA Gateway Module .....	11-2
Installing the VGM .....	11-3
Step 1 - Mount the VGM.....	11-3
Step 2 - Connect the VGM .....	11-4
Step 3 - Add and set up the VGM .....	11-6

Step 4 - Auto enroll the VGM .....	11-7
Step 5 – Enable the VGM in the VISTA FBS .....	11-12
Step 6 - Configure the VGM .....	11-13
Defining Test Report Schedules and VGM Interface.....	11-14
Defining VISTA Zones .....	11-16
Defining the Default VISTA FBS User Number.....	11-20
Step 7 - Download the database .....	11-22
<b>Adding System Modules .....</b>	<b>12-1</b>
Understanding System Modules .....	12-2
Installing Modules .....	12-3
Adding and Enrolling Modules.....	12-3
Adding a module .....	12-3
Enrolling a module .....	12-5
Configuring Modules .....	12-10
DCM setup dialog box.....	12-11
QRM setup dialog box.....	12-12
QRM system tab .....	12-13
Relay tabs .....	12-14
Trigger tabs.....	12-16
CPM setup dialog box .....	12-17
CPM System tab .....	12-18
Reader tab .....	12-18
User Terminal tab .....	12-20
VGM setup dialog box .....	12-20
ZIM setup dialog box .....	12-21
ZIM System tab .....	12-21
ZIM Zone tabs .....	12-22
Download the Database .....	12-24
<b>Wiring Considerations.....</b>	<b>A-1</b>
Wiring Considerations .....	A-2
Topology.....	A-2
Wiring notes .....	A-7
Wire characteristics .....	A-8

Main Logic Board Connections .....	A-9
Door Control Module Connections.....	A-10
Power Supply Specifications .....	A-11
<b>Firmware Download .....</b>	<b>B-1</b>
Downloading MLB Firmware.....	B-2
Downloading Account Information .....	B-10
<b>Wiring Reference.....</b>	<b>C-1</b>
Null Modem Cable.....	C-2
Extension Cable .....	C-3
Modem Cable.....	C-4
Door Expansion Kit .....	C-5
Card Enrollment Kit.....	C-6
VISTA Gateway Module .....	C-7
Main Logic Board.....	C-8
Door Control Module.....	C-9
Power Supply .....	C-10
<b>Access Control Glossary .....</b>	<b>G-1</b>
<b>Access Control Index .....</b>	<b>I-1</b>



# *Section One*



## *Setting Up PassPoint*





## Chapter

# 1

## *Introduction to Setup*

This chapter provides you with an overview of the various PassPoint Access Control Kits. It also provides a full description of the PassPoint Access Starter Kit and the steps involved in getting your system installed and configured.

In this chapter you will learn about:

- **The contents of this section**
- **The contents of your PassPoint Access Starter Kit**

## ***Understanding PassPoint Kits***

This guide is about PassPoint Kits, the basic pre-configured PassPoint packages you will use to quickly get your system up and running. All kits are self-contained. By combining kits (and separate PassPoint modules), you can expand and build on any existing PassPoint installation.

There are four types of PassPoint kits:

- **Basic Starter Kit (BSK)**

The BSK contains everything except card readers and cards that you need to get a two-door installation up and running. This kit is designed primarily for retrofit installations.

- **Access Starter Kit (ASK)**

The ASK contains everything you need to get a two-door installation up and running. It is the basic building block of most PassPoint systems. Most of this guide describes the ASK.

- **Door Expansion Kit (DEK)**

The DEK allows you to add two more doors to an already operational PassPoint system. The components of the DEK, as well as installation and configuration instructions, are provided in the “Adding a Door Expansion Kit” chapter of this guide.

- **Card Enrollment Kit (CEK)**

The CEK is a kit that allows you to quickly enroll system ID cards. It consists mainly of a stand-alone card enrollment reader that connects directly into your existing system. Installation and configuration instructions for the CEK are provided in the “Adding a Card Enrollment Kit” chapter of this guide.



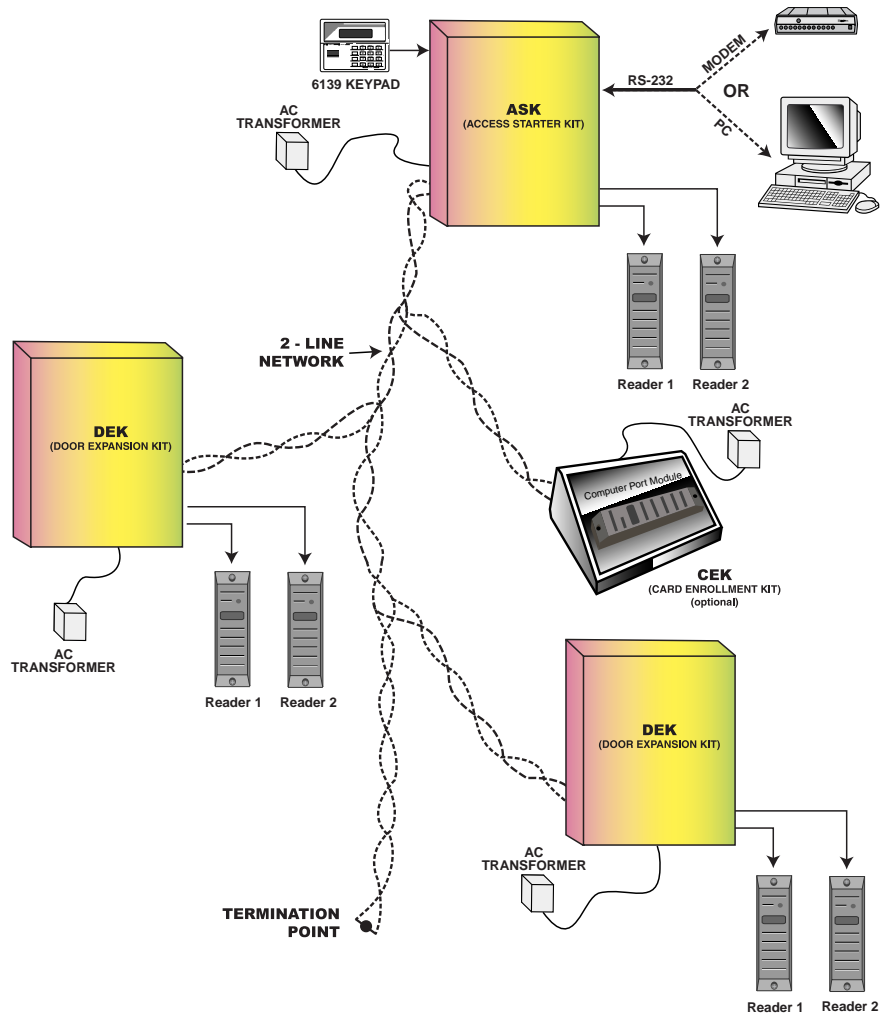
---

In addition to these kits, you can also add individual system modules to a PassPoint system. For information about individual modules, refer to the “Adding System Modules” chapter of this guide.

---

## ***System Hierarchy***

The PassPoint system is composed of kits. Shown below is an example of a basic PassPoint installation:



## What's In Section One?

Section One of this guide contains everything you need to get your PassPoint Access Starter Kit up and running. It walks you step-by-step through all the procedures from installing your hardware to enrolling some test ID cards. Once you have enrolled some test cards, you can test your system to see if it is running properly. When installing the Basic Starter Kit, follow the procedures for the Access Starter Kit. Items not applicable to the Basic Starter Kit are noted at the points they apply within this guide.



---

This section has been written from the perspective of a two-door system only. If you have purchased a PassPoint Door Expansion Kit or Card Enrollment Kit, refer to Section Two of this guide for complete instructions on installing and configuring these kits.

---

This section of the guide has been divided into four parts:

- **Part One - Preparing for Your Installation**

Before attempting to install the PassPoint system, there are several preparations you should make. Proper preparation will make the task of installing the system much easier. Chapter 2 tells you how to prepare for your installation.

- **Part Two - System Installation**

Chapter 3 is the system installation section of this guide. This section tells you how to connect all of the system modules that come with your kit, including mounting the cabinet and wiring your card readers.

- **Part Three - PassPoint *Plus* Installation**

PassPoint *Plus* is the system software you will be using to configure and operate your PassPoint system. It must be

installed on your user computer (i.e., the PC you will be using to connect to the system's panel). Chapter 4 covers the entire installation of PassPoint *Plus*.

- **Part Four - System Configuration**

After you have installed your system hardware, you must configure the system so that it will operate properly. Most configuration options for your PassPoint Starter Kit have already been defaulted at the factory, but there are some configuration options that still need to be set by you, such as setting up your doors and enrolling access cards.

Configuration information begins in Chapter 5.

## ***About Your PassPoint Access Starter Kit***

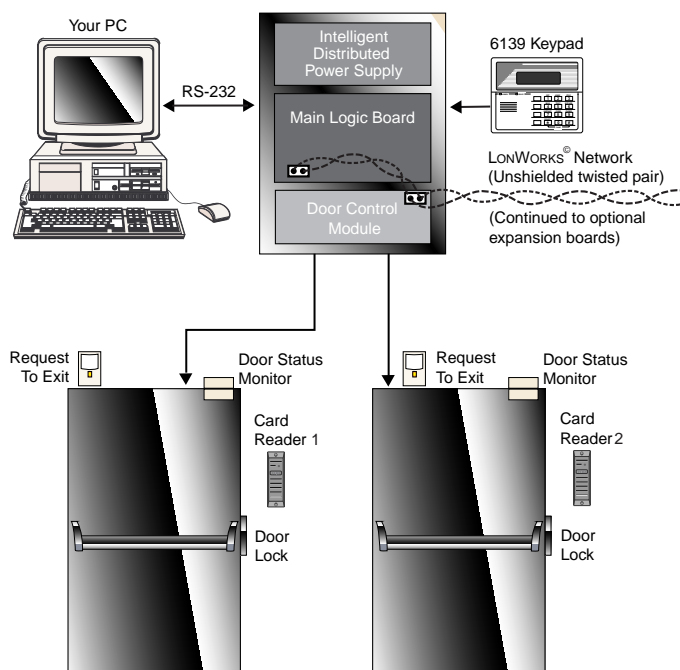
The PassPoint Access Starter Kit (ASK) is designed to be easy to install and configure. Where possible, default configuration options have been provided. If you follow the procedures in this guide, you should have no trouble getting your system operational.

### ***What's in your kit?***

Your Access Starter Kit consists of the following hardware components:

- 1 pre-configured access panel, consisting of the following:
  - 1 metal enclosure
  - 1 Main Logic Board
  - 1 Door Control Module
  - 1 power supply
- 1 plug-in transformer
- 2 mullion-mount proximity readers (ASK only)
- 1 ADEMCO 6139 keypad

- ID cards (ASK only)  
(For use with card readers)
- PassPoint *Plus* software
- 1 RS-232 cable (null modem cable)  
(Used for connecting your PassPoint panel to your user computer serial port)



**Access Starter Kit in  
typical system configuration**



## **Major components**

There are four main components to your PassPoint system. They are:

### ***Main Logic Board (MLB)***

The MLB is the central controller of the PassPoint 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 PassPoint power supply, and communicates with the Door Control Module (described below) to determine if access should be granted at a particular access point.

### ***Door Control Module (DCM)***

The DCM provides all the inputs and outputs required to manage two access points (i.e., doors). The DCM can connect to two card readers and simultaneously accept card data from two card readers. It provides two Form C, supervised output (i.e., voltage-monitored) relays that are used to operate electromagnetic door locks or door jamb-mounted lock strikes. It also provides two trigger outputs that can be used to operate sounders or LEDs.

### ***The PassPoint system power supply***

The PassPoint system 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 (supplied with your kit). The power supply provides a battery backup/charger connection and supports a 7AmpHour battery (not supplied).

Connection information and specifications for the power supply are in Appendix A.



### ***The PassPoint Plus system interface***

PassPoint *Plus* is a Windows 95, Windows 98, and Windows NT 4.0 compatible software program that allows the computer to communicate with the Main Logic Board of the system. You will use PassPoint *Plus* to configure the system. After the system is up and running, the system operators will use PassPoint *Plus* to operate PassPoint.



---

The PassPoint *Plus* system interface requires a computer. The computer is used to configure and operate the system, although the computer is not necessary for the system to run unattended. Also, if you are running PassPoint *Plus* remotely, you will need two modems to connect the computer with the PassPoint system. Both the computer and modems are considered accessories and are not included with your PassPoint Access Starter Kit.

Refer to the “System Requirements” section of Chapter 4 for more information.

---

## ***Installation and Setup Map***

Below is a depiction of all the steps that must be taken to get your PassPoint system up and running. The steps are broken down into parts. Each part is covered in detail in a different chapter of this guide.



## ***Where do you go from here?***

Begin by preparing for your installation. Instructions for preparation are included in the next chapter. Here you will see how to use a floor plan to determine your system layout, and will be prompted with some important questions that must be considered before you can proceed with installing your system.



## Chapter

# 2

## *Preparing for Your Installation*

Before attempting to install the PassPoint system, there are several things you should do to prepare for your installation. Proper preparation will make the task of installing the system much easier.

In this chapter you will learn:

- **How PassPoint can be installed to suit your individual needs**
- **How to select and configure the access points for your system**
- **How to place your system components**
- **What steps must be performed for hardware installation**



## ***How Should You Prepare for Your Installation?***

With PassPoint, proper preparation is essential to a sound, problem-free installation. It requires knowing your site and its access points, and knowing the level of security desired for each point. It also requires the proper placement and utilization of system hardware.

Because the system is so flexible, you can install its components in multiple ways. There are, however, several things common to each installation, such as access points and hardware. These common configuration issues are a good place to start when preparing for your own installation.

### ***Understanding access points***

PassPoint defines access points beyond the conventional definition of a simple door. An access point represents a collection of objects (i.e., resources) that allow entry/egress through a portal. These objects include the hardware-related items (readers, locks, etc.) as well as software functions that parameterize the access point (schedules, cardholders, etc.).

## ***Ask Yourself Some Basic Questions***

A good approach to preparing for your installation is to ask questions about the site into which PassPoint is being installed. Answering these questions will help you determine the type of hardware you need, where it should be placed, how it should be wired, etc. Then, after you've installed and wired your system hardware, you will be able to configure it using one of the system's interfaces.

Below are some of the questions that you will need to answer before you can begin your installation. It should be noted that these questions pertain to a general installation. Because of the flexibility of PassPoint, it is impossible to foresee and describe every possible installation scenario. But when used as a general guide, the answers to these questions will have you well on your way to a successful PassPoint installation.

### ***Question 1 - Where will my access points be?***

This is perhaps the most important consideration when preparing for your installation. Access points, or doors, control the entry and egress from a premises, as well as the flow of traffic within the premises. You must determine which doors you want to control.

See the section of this chapter titled “*Selecting Your Access Points*” for instructions on choosing your system’s access points.

### ***Question 2 - What level of security should I have for my access points?***

Security levels for access points can vary, depending on what type of system hardware the access point has and how it is configured. You can have a door with only a card reader, or with a card reader/keypad combination. The door can be monitored for its status, or it can simply be allowed to stay open unconditionally. Many other security level options are also available.

See the section of this chapter titled “*Selecting Your Access Points*” for information regarding access point security levels.

### ***Question 3 - What type of door control hardware should I use?***

The type of door control hardware you should choose depends in part on the level of security you want for each access point. As



stated above, you can have doors equipped with only a single card reader, or you can have card reader/keypad combination units requiring an occupant to enter a PIN code and swipe his/her card. There are many types of door control hardware available, as well as different ways to configure them.

#### ***Question 4 - Where will my system computer be located?***

You must determine where the computer running your system software will be located keeping in mind that any one RS-232 connection should not exceed 50 feet. You are not limited by physical distance, as the Main Logic Board of the system can communicate to your system interface via modem as long neither the system/modem or modem/computer RS-232 cable exceeds 50 feet.

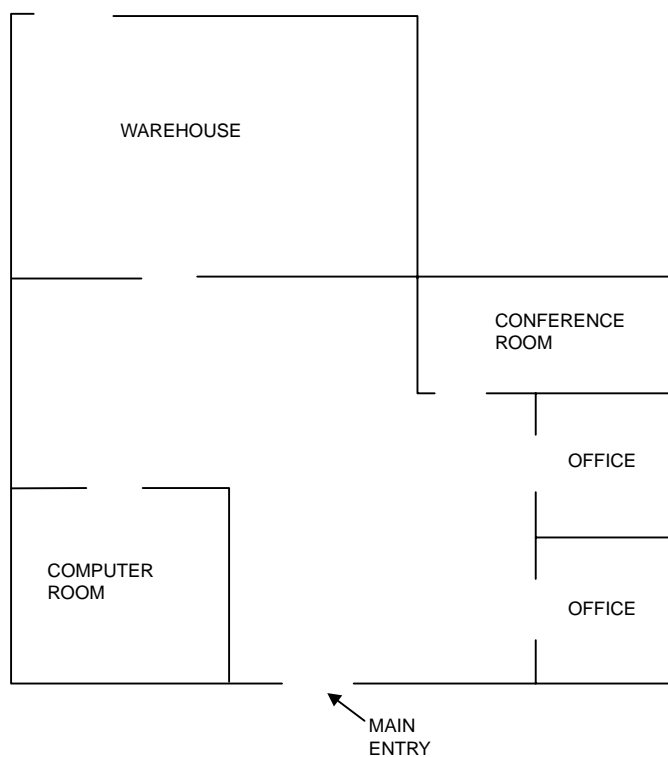
### ***Use a Floor Plan***

When you prepare for your PassPoint installation, we strongly recommend that you obtain a floor plan of the installation premises, if possible. A floor plan allows you to visualize your installation and helps you to determine your access points and hardware locations. A floor plan can be any blue print or design plan showing the “foot print” (i.e., the top view) of the premises.

If you are unable to obtain a floor plan of the premises, you can simply draw one yourself. It doesn't have to be anything elaborate, just a simple aerial view of the building showing its doors and rooms scaled to their approximate dimensions. Dimensions are important because there are wire length considerations that must be kept in mind when wiring together the system hardware.

Here is an example of a simple floor plan:

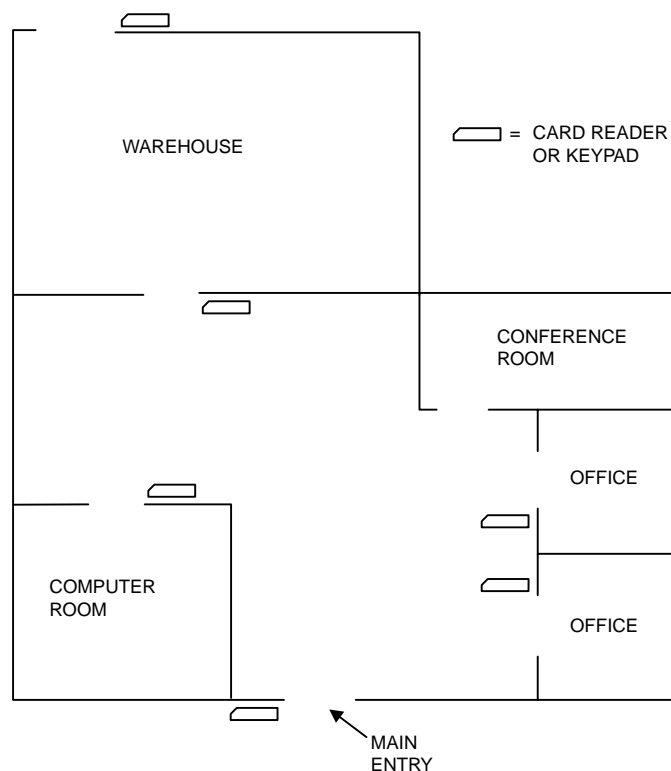
*Here's a business office without PassPoint installed. Note that every room is accessible to everyone.*



Of course, your own floor plan may be much more extensive than this one, but the principles involved are the same. You have a premises with a main entry/exit door, and the premises contains other rooms and facilities that must also be protected.

Now with this floor plan in hand, you can decide what you want to protect and how to do it:

*That same premises with PassPoint installed now controls the flow of people between rooms.*



In the case of this PassPoint installation, you can see that most of the rooms have been protected with a card reader (or keypad). The conference room, however, has been left unprotected by the PassPoint system, as it needs to be accessed by everyone at any given time. It should be noted again that although the floor plan above shows the use of card readers or keypads, these devices could just as easily be combination (card reader with keypad) units.

## **Selecting Your Access Points**

The first step in preparing to install your PassPoint system is to select your access points. Simply put, access points are the doors that people will use to enter and exit the premises being controlled. Once you've chosen what doors you want monitored, you can then decide the level of access control you want for each. This will determine the type of hardware needed for each access point.

### ***Access point configurations can vary***

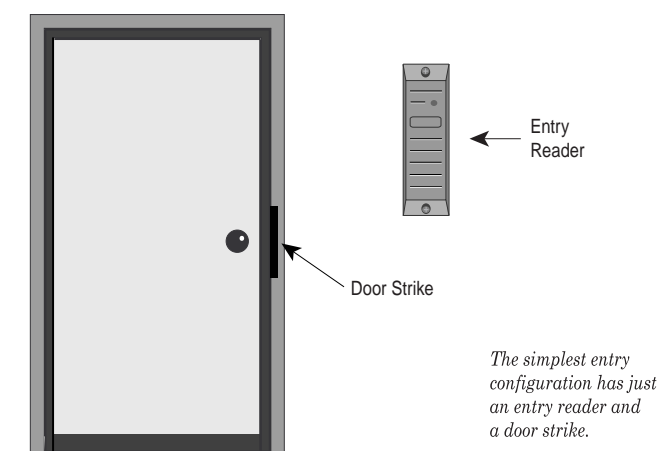
Each access point can be configured in several different ways. Each way provides a different degree of security and can enforce a direction of passage through the access point.

Remember that an access point is really a combination of system resources (i.e., card readers, door control relays, and protective zones). The way you combine these resources determines the level of security for the access point. It also determines whether the access point is a Door Status Monitor (DSM) zone or a Request-to-Exit (RTE) zone. DSM and RTE are the two kinds of protective zones. An access point can be one of these zone types, both types, or neither.

Below are some sample access point entry control configurations. They range from very simple (and consequently less secure) to fairly elaborate.

### **Example 1 - Basic entry control**

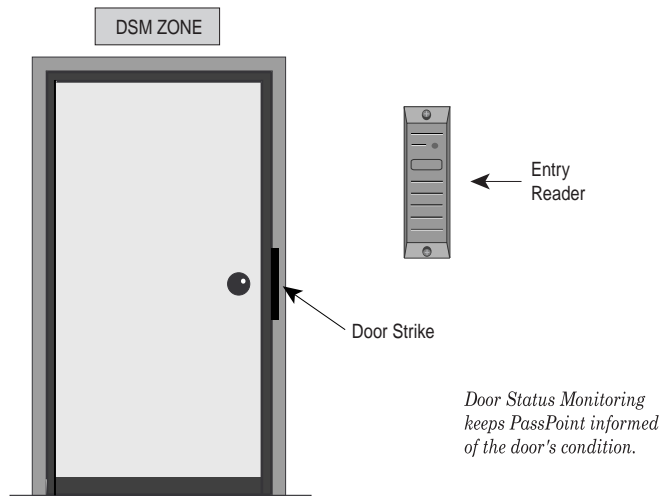
The simplest configuration for entry control is to have an entry reader and a door control relay positioned at the access point:



In this configuration, the cardholder swipes his/her ID card at the card reader to gain entry to the access point. The reader reads the data on the card and PassPoint determines whether or not to grant access to the cardholder. If access is granted, the door control relay at the access point is energized and the door strike is unlocked, allowing the cardholder to enter.

## ***Example 2 - Entry control with Door Status Monitoring***

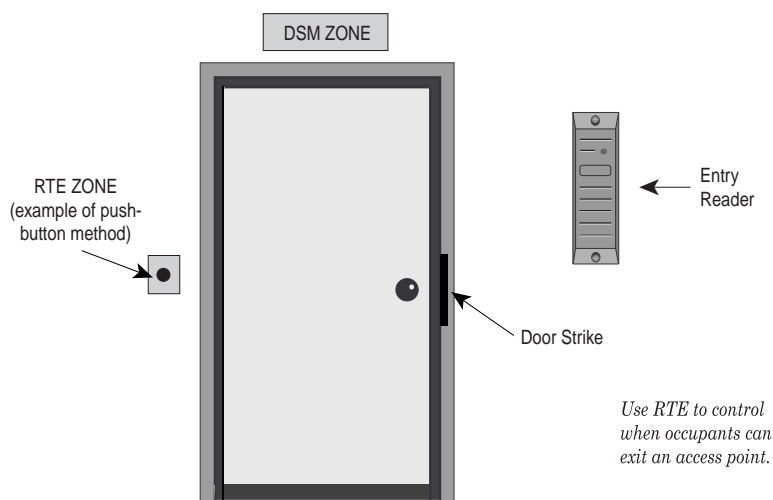
Here is the same configuration as Example 1, only with Door Status Monitoring added:



As its name implies, Door Status Monitoring allows the system to constantly monitor the access point for any change in its status. It lets the system know when the door has been forced open or when it has been held open longer than normal after access has been granted. Without DSM, as in Example 1, the system only determines whether or not to grant access. It does not monitor the status of the access point for anything unusual.

### **Example 3 - Entry control with Door Status Monitoring and Request-to-Exit**

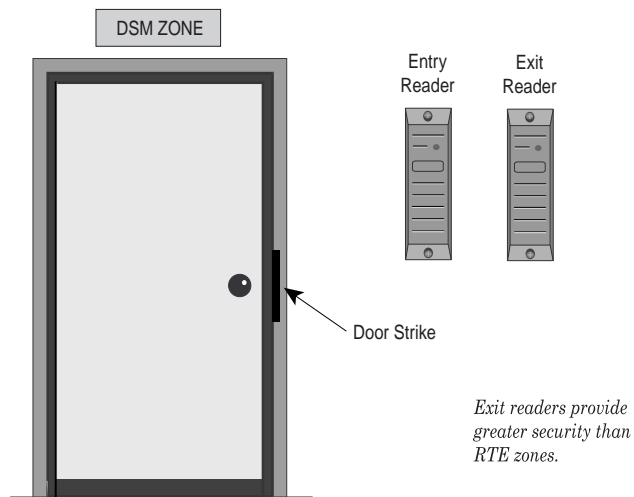
Add Request-to-Exit to an access point and you can control when to allow occupants to exit:



RTE zones allow the system to understand when the access point's door is to be unlatched so that an occupant may exit. The device used for RTE can be a button that the occupant must push to exit, or it can be an infrared motion detector that automatically detects when an occupant is near the door. In either case, the device is always mounted on the protected side of the access point.

### ***Example 4 - Entry and exit control with Door Status Monitoring***

For added security, an exit reader can be added to the access point:



When an access point has an exit reader, occupants must “swipe out” in order to exit. That is, they must show the system their card again. Unlike the RTE zone described in Example 3, this configuration directs the system to be very selective about who is allowed to exit. Only occupants with a valid ID card may exit through the access point.

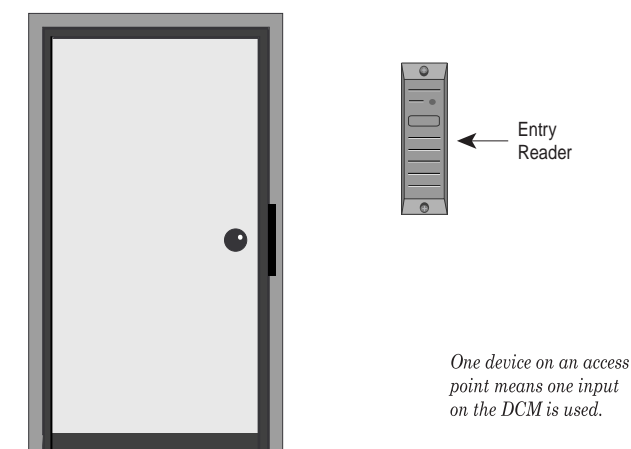


## ***Door Control Module configuration***

Because each DCM has inputs and outputs for only two devices (i.e., card readers, keypads, or combination units), these limitations must be kept in mind when planning your installation.

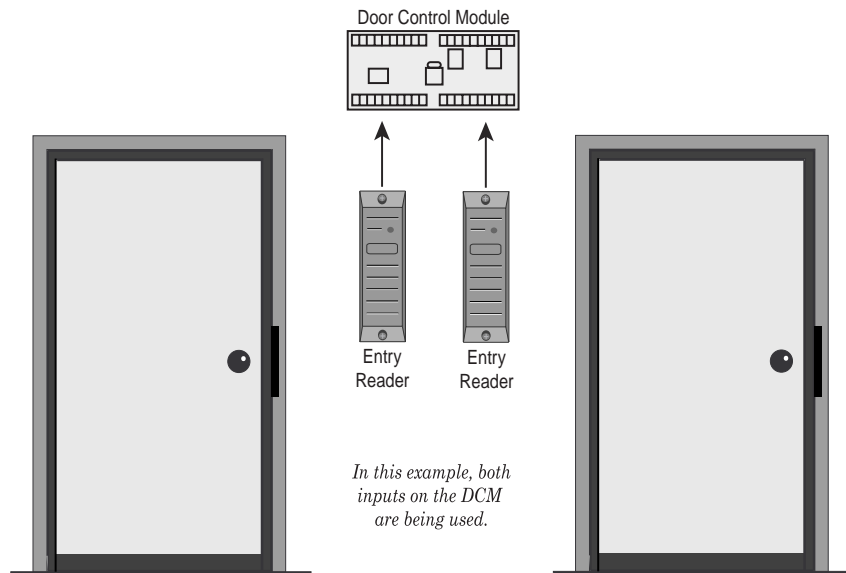
Specifically, which doors do you want to control and how do you want to control them?

Consider again the access point examples given in the previous sections. In the first example, we have a basic entry control system with a single card reader:



In this example, as there is only one reader assigned to the door, the DCM used for the access point still has one input remaining.

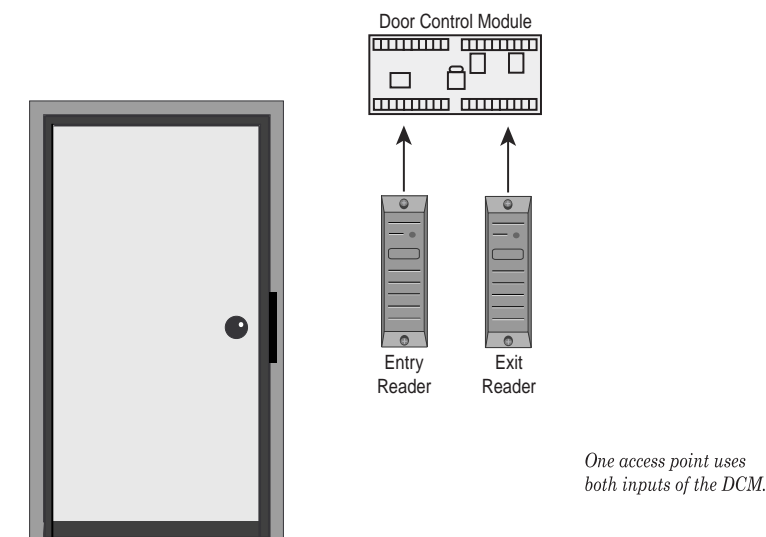
Therefore, this DCM can be used to manage another door (provided that door also has only one device), as in the diagram below:



If an access point has two readers on it, both inputs of the DCM are required. There are a number of times when this will be the case, and you must be aware of them in order to plan your installation properly.

*For example, if you have an access point that requires both an entry reader and an exit reader, you must wire both devices to the inputs of the DCM. This requires using the entire input capacity of the DCM for one access point.*

This example is illustrated below:



When you install your DCMs, remember the limitations described above. Knowing how DCMs can be configured directly relates to how many DCMs you will need and where to position them.

## Types of Card Readers

With PassPoint, there are several types of card readers that can be used throughout the system. You have already seen two of the reader types (entry readers and exit readers) in the examples in the previous section. Each PassPoint reader type is explained below:

**Entry readers** - These readers are used to control entry to an access point. The cardholder swipes his/her card at the reader to

gain entry. The reader reads the data on the card and the system determines if access should be granted. If access is granted, the door is unlocked for a specified period of time (defined by the installer) and the cardholder can open the door.

**Exit readers** - Exit readers work nearly identically to entry readers, except that they are used to control egress from an access point.

**Command readers** - These readers are used to perform specific functions, or “commands.” For instance, a command reader might be positioned in a building’s front hall within easy reach of someone coming through the front door. When the cardholder swipes his/her card at the reader, the lights for the building might go on. The card swipe does not unlock the door. Instead, an event/action relationship has been set up between the card and the reader.

**Enrollment readers** - These readers are used to enroll new cards into the system. Cards can be added individually or in a batch using an enrollment reader.

All card readers, no matter what their function in the system, connect directly to Door Control Modules. The only exception to this is enrollment readers. Enrollment readers can connect to a Door Control Module, or they can in a Card Enrollment Kit (CEK). The CEK has a built-in card reader used specifically for card enrollment.

The function that a reader performs is set during module configuration after the reader has been connected to a DCM. When you configure a DCM, the system asks you about the reader(s) connected to the module. You then tell the system which function you want the reader to perform.

***Committed and  
uncommitted  
readers***

All readers, no matter what their function, fall within two main categories: committed and uncommitted.

- **Committed Readers**

Committed readers are readers directly associated with access points. That is, they control entry or exit through a door. These readers can be straight entry readers, entry with door status monitoring, straight exit, etc. The committed reader is the most common type of reader in an installation, and is the one that most cardholders will be familiar with. The cardholder swipes his/her card at a committed reader to gain entry or egress through a door.

- **Uncommitted Readers**

Uncommitted readers are NOT associated with access points. Although they connect to DCMs just as committed readers do, they do not control entry or egress through doors. Uncommitted readers can either be command readers or enrollment readers. CEK/CPM readers are always uncommitted readers.

## ***Where do you go from here?***

Now that you have made the proper preparations, you can begin installing your system. Full instructions for installing your system are included in the next chapter. Here you will see how to mount the PassPoint panel and make all the connections necessary for your system to function properly.



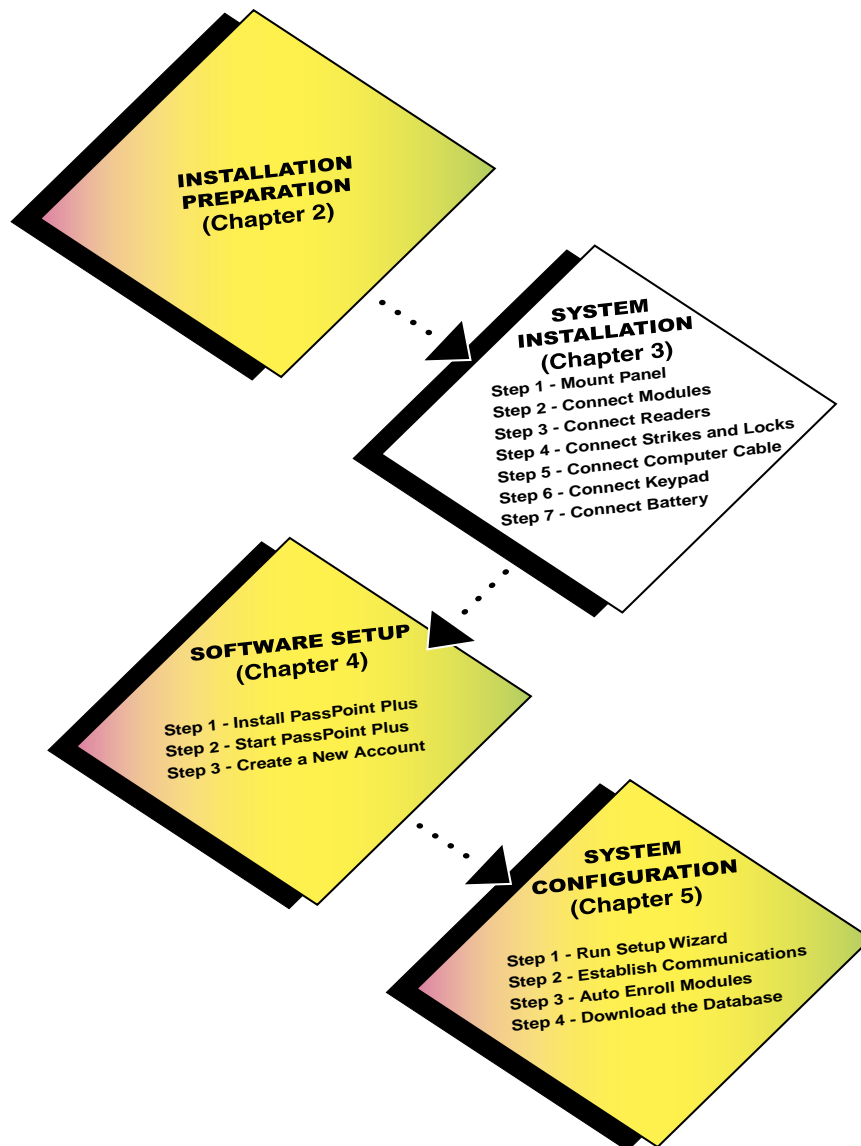
## Chapter

# 3

# *System Installation*

This chapter shows you how to install and wire your PassPoint system. In this chapter you will learn how to:

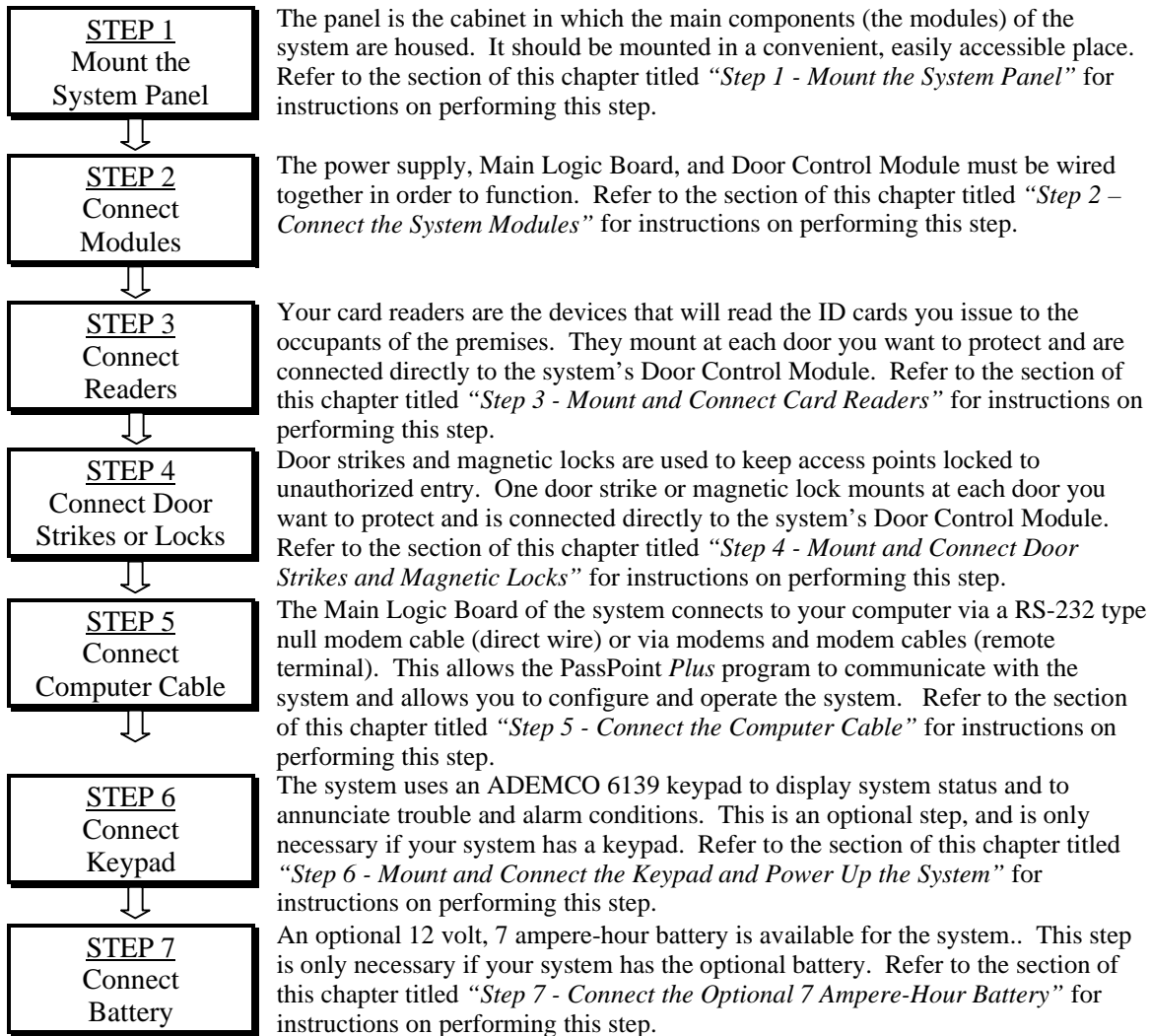
- **Mount the system panel**
- **Connect your card readers**
- **Connect your door strikes or magnetic locks**
- **Connect the system's computer cable**
- **Mount and connect the system keypad**
- **(Optional) Mount and connect the 7 ampere-hour battery**





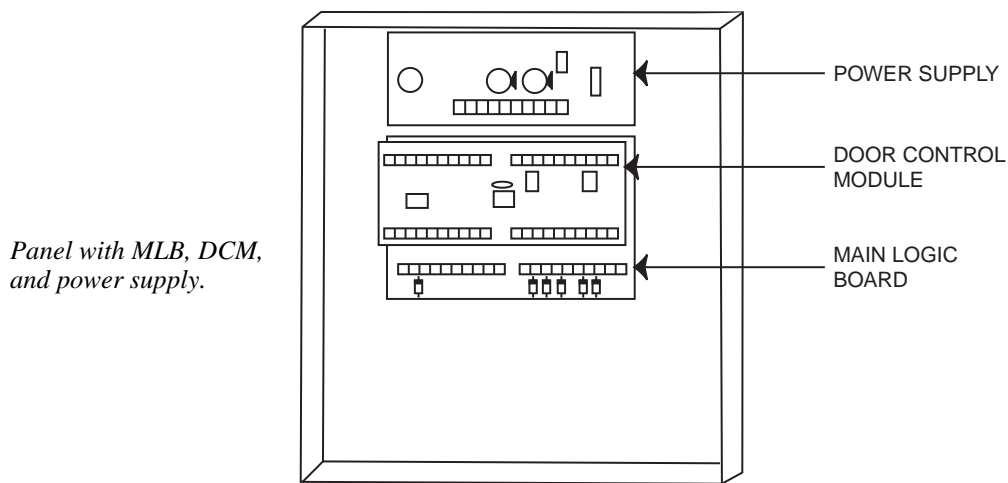
## Summary of Installation Steps

Below is a list of all the steps you must perform in order to install your PassPoint system. Each step is covered in detail in this chapter. Follow each step in order, referring to the applicable section of this chapter:



## ***Step 1 - Mount the System Panel***

The ASK panel (or cabinet) contains all of the modules of the PassPoint system. All of the modules have been pre-mounted and await cabling. When the door to the panel is removed, the inside of the cabinet looks like this:



### ***Choosing a mounting area***

When selecting a mounting area for the panel, choose a clean, dry place not readily accessible to the general public but convenient enough so that a technician can get at the panel easily. The panel should be mounted on a sturdy wall using fasteners or anchors (not supplied in your kit). Also, the panel should be mounted near a suitable AC outlet and the system's computer. Refer to Appendix A of this guide for applicable wiring distance parameters.

To mount the panel, follow the procedure below:

- 1. Position the cabinet on the wall and use the holes in the back of the cabinet to mark your four mounting holes.**
- 2. Using four anchors or fasteners, mount the cabinet to the wall.**



---

When mounting the cabinet, be very careful not to jar the system's PC boards.

For ease of installation, seven removable terminal blocks, ADEMCO 4142BLK, have been included with the kit.

---

## ***Step 2 - Connect the System Modules***

Connecting the system modules within the cabinet actually involves three steps:

- **Connecting the MLB to the power supply**
- **Connecting the DCM to the MLB and power supply**
- **Connecting the MLB ribbon cable**



---

When making these connections, refer to Appendix A, Wiring Considerations, for diagrams and system ratings.

---

**Connecting the  
MLB to power  
supply**

1. **Connect the leads of the wall pack power transformer to terminals 1 and 2 of the power supply.**
2. **Connect the local power jumper between power supply connector J1 and MLB connector J1.**

This is the most common way of connecting the MLB to the power supply. However, if you do not want to use the jumper, you can connect the local power from the power supply to the MLB using wire runs between the terminal strips.



---

Do not plug the transformer in until all other wiring connections are made.

When making all system connections, be sure that leads are secure in their terminals and not frayed or touching other components on the panel.

---

**Connecting the  
DCM to the MLB  
and power  
supply**

1. **Connect the *remote* power jumper between power supply connector J5 and DCM connector J1.**

Remote power supply power (i.e., J5) is used for powering DCMs when the DCM is mounted in a cabinet with a Main Logic Board.

2. **Connect two network connection leads between the MLB and DCM.**

Connect one lead between terminal 1 of the DCM and terminal 16 of the MLB.

Connect the other lead between terminal 2 of the DCM and terminal 15 of the MLB.

Note that the system is polarity-insensitive. On the network, you may connect either terminal 1 or 2 of the DCM to either terminal 15 or 16 of the MLB, then connect the other DCM terminal to the remaining MLB terminal. Be sure to install a termination resistor on the network. You may use either a

single 52.3 ohm resistor across terminals 15 and 16 of the MLB, or two 105 ohm resistors, one across MLB terminals 15 and 16 and the other across DCM terminals 1 and 2.



Use twisted pair wiring for these connections. Also, use proper termination for the modules. Refer to Appendix A for details about wiring considerations for larger systems.

### **Connecting the MLB ribbon cable**

The system comes with a nine-pin ribbon cable used to connect the MLB to the computer cable. One end of this cable gets connected to the MLB. The other end gets mounted onto the cabinet, so that the computer cable can be plugged into it.

- 1. Connect the RS-232 ribbon cable to connector J2 on the right side of the MLB.**

The RS-232 ribbon cable allows communication between the MLB and the system computer.

- 2. Secure the other end of the ribbon cable (i.e. the 9-pin “D” connector) to the right side of the cabinet using hardware supplied.**

## **Step 3 - Mount and Connect Card Readers**

Your PassPoint Access Starter Kit comes with two card readers. Each card reader is mounted near an access point (i.e., door) and is wired directly to your system’s Door Control Module (DCM). A single DCM has input connections for two readers. Therefore, one DCM can control two doors, each with a single reader.

First, mount your readers at your access points. After they have been mounted, connect them to your DCM. The instructions for performing both procedures are included in this section.

---



Specifications and connection information for the PassPoint power supply are in Appendix A at the end of this guide.

---

### ***Mounting card readers***

1. Using the reader as a drilling template, drill two mounting holes and one cable hole in each mounting wall for the readers.
2. Using the reader mounting hardware included with the readers, secure the readers to the wall.

### ***Connecting card readers***

Once the card readers are mounted, connect them to the system as follows:

1. **Wire the leads from card reader #1 to the applicable terminals of the DCM.**

Use the chart below to connect the leads from the card reader to the specified terminals of the DCM.

Lead from Reader 1	Lead Color	To DCM Terminal #
Green LED (RdrA)	(See Note 1)	11
DATA 1 (Data)	White	12
DATA 0 (Clock)	Green	13
Ground	Black	14
+5VDC	Red (See Note 2)	15
+12VDC	Red (See Note 2)	16
NOTES: 1. Use orange lead for Green LED signal on some HID readers. All other readers use brown lead. Check the label on your reader for proper connection. 2. Connect to +5VDC or +12VDC per reader manufacturer's specification.		



The readers included with the kit have nine leads, but only five of them are used and need to be wired. The other four leads are not used and do not need to be connected. The unused wires must be insulated from each other and any other wires or conductive material.

## 2. Wire the leads from card reader #2 to the applicable terminals of the DCM.

Use the chart below to connect the colored leads from the card reader to the specified terminals of the DCM.

Lead from Reader 2	Lead Color	To DCM Terminal #
+5VDC	Red (See Note 1)	15
+12VDC	Red (See Note 1)	16
Ground	Black	17
Green LED (RdrB)	(See Note 2)	18
DATB 1 (Data)	White	19
DATB 0 (Clock)	Green	20
NOTES: 1. Connect to +5VDC or +12VDC per reader manufacturer's specification. 2. Use orange lead for Green LED signal on some HID readers. All other readers use brown lead. Check the label on your reader for proper connection.		



Refer to Appendix A for proper wire-run lengths.

## ***Step 4 - Mount and Connect Door Strikes and Magnetic Locks***

Door strikes and magnetic locks are used to keep access points locked against unauthorized entry. One door strike or magnetic lock mounts at each door you want to protect. Door strikes and magnetic locks receive their power from the PassPoint power supply through the output relays of the DCM.





The PassPoint Access Starter Kit does not ship with door strikes or magnetic locks. PassPoint can support most types of door locking hardware compatible with the system's power supply specifications. This hardware can be purchased from any reputable dealer of security hardware.

Also, be sure to keep any documentation accompanying this hardware. You will need to refer to it for mounting and connection information.

---



It is absolutely necessary to use an electric suppressor such as EL-EDS (manufactured by EDCO) to provide transient protection for magnetic locks/door strikes and relay contacts. Install a suppressor across the leads connected to the lock as close as possible to the lock and install a second suppressor across the relay connection on the DCM.

---

### ***Mounting door strikes and magnetic locks***

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

### ***Connecting door strikes and magnetic locks***

To connect a door strike or magnetic lock, follow the procedure below and refer to the Connection diagrams in Appendix A.

#### **1. Wire the *door strike output* of the power supply to the common terminal of the DCM output relay.**

The door strike output of the power supply is terminal #7.

The common terminal of the DCM output relay is terminal #29 for door A, terminal #24 for door B.

2. **Wire the normally open (N.O.) or normally closed (N.C.) terminal of the DCM relay to the door strike or magnetic lock. A minimum distance of 6 inches must be maintained between the door strike wiring and any other wire for the length of the wire.**

If you are wiring a door strike, use an N.O. terminal. The N.O. terminals are #28 for door A, #23 for door B.

If you are wiring a magnetic lock, use an N.C. terminal. The N.C. terminals are #30 for door A, #25 for door B.

3. **Wire the door strike or magnetic lock to the ground terminal of the power supply (terminal #8). A minimum distance of 6 inches must be maintained between the door strike wiring and any other wire for the length of the wire.**
- 



Refer to Appendix A for proper wire-run lengths.

---

### ***Connecting DSM and RTE devices***

Zones A through D of the DSM (terminals 5 through 10) can be used for optional Door Status Monitoring (DSM) or Request-to-Exit (RTE) devices.

Connect these devices according to the DCM summary of connections diagram. Also, refer to Appendix A of this guide for applicable wiring information, and Chapter 12 for a description of the different possible zone configurations.

## ***Step 5 - Connect the Computer Cable***

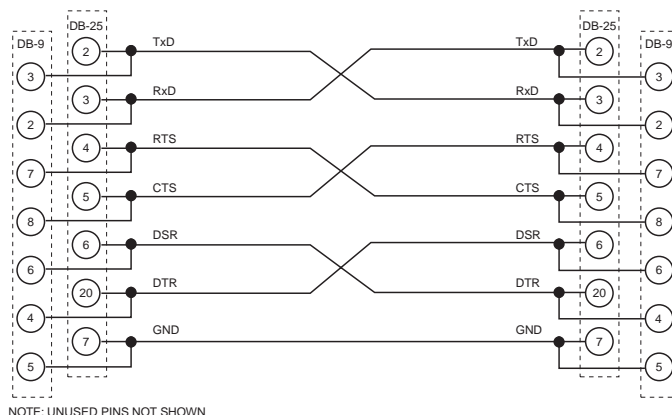
The PassPoint panel may be connected directly to your system interface via an RS-232 cable (hardwire connection) or via modem cables, modems, and a telephone line when your panel is at a different location than the computer (remote terminal connection).

### ***Hardwire Connection***

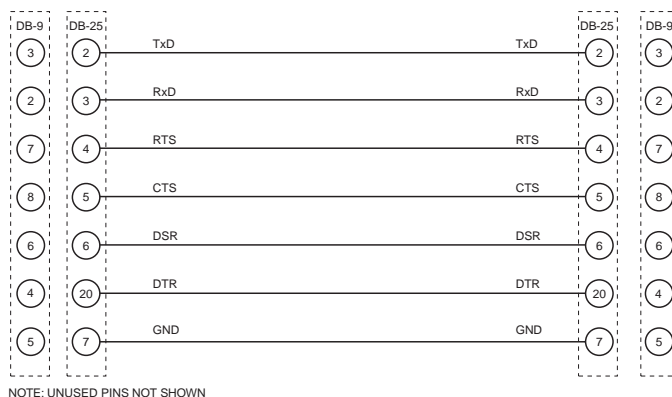
The PassPoint panel connects to your system computer (i.e., PC) via an RS-232 cable when using a hardwire connection. The cable goes from the PassPoint system to an available COM port on your computer.

If you intend to use a longer cable than the RS-232 cable supplied, you must purchase or make a “null modem” cable or extension cable to be used with the supplied null modem cable. The null modem cable or extension cable must be wired as shown in the following illustrations.

**NOTE:** The total length of the cable(s) between the PassPoint panel and computer should not exceed 50 feet.



## NULL MODEM CABLE



## EXTENSION CABLE

To connect the RS-232 computer cable:

1. **Connect the 9-pin “D” connector to the PassPoint panel.**
2. **Connect the other end of the cable to an available COM port of your computer.**

Write down the COM port number you are using for the PassPoint system. You will need to know the COM port number when you configure your system.

MLB RS-232 Port J2	Description	DB-9 Male Connector on side of Cabinet
Pin 1	DCD IN	1
Pin 2	DSR IN	6
Pin 3	RXD IN	2
Pin 4	RTS OUT	7
Pin 5	TXD OUT	3
Pin 6	CTS IN	8
Pin 7	DTR OUT	4
Pin 8	RI IN	9
Pin 9	Ground	5
Pin 10	N/C	N/C

### ***Remote Terminal Connection***

The PassPoint panel connects to your system computer (i.e., PC) via 2 modems, a telephone line connection, and 2 DB-9 to DB-25 modem cables when using a remote terminal connection. At the PassPoint panel location, a modem cable goes from the PassPoint panel to a modem. At the terminal location, a modem cable goes from the modem to an available COM port on your computer.

Compatible cable numbers and modems are as follows:

- DB-9 to DB-25 Modem Cable - ADEMCO Part Number N8337
- Hayes Accura, US Robotics Sportster, or compatible 28.8kbs (or faster) modems



---

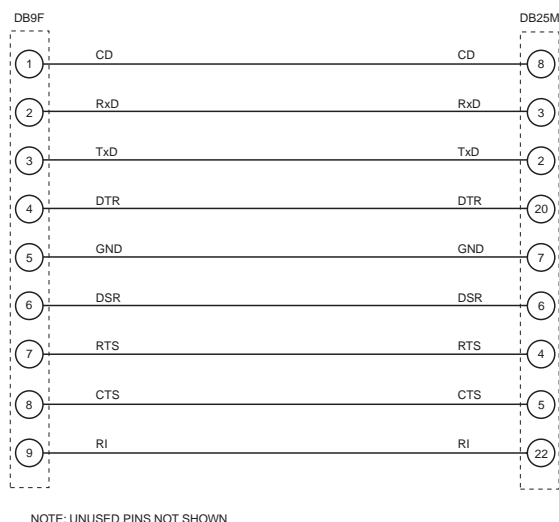
The modem and modem cables are not supplied as part of the Basic Starter Kit or Access Starter Kit. The modem and modem cables must be purchased separately.

---

If you intend to use a longer cable than the ADEMCO modem cable, you will need to purchase a modem cable from another source or make a modem cable. The modem cable must be wired as shown in the following illustration.

**NOTES:**

- The total length of the cable(s) between the PassPoint panel and modem or the modem and your computer should not exceed 50 feet.
- External modems, which have DB9F (9-pin female) connectors, can use a straight-through (one-to-one) 9-pin male-female cable. Each of the 9 conductors is connected to the same pin number on each side.



## MODEM CABLE

To connect the PassPoint panel to the computer:

### *At the PassPoint Panel location*

1. Connect the 9-pin modem cable connector to the PassPoint panel.
2. Connect the other end of the cable to the modem.
3. Connect the modem to the telephone jack.

### *At the Computer location*

1. Connect the modem to the telephone jack.
2. Connect the 25-pin modem cable connector to the modem.
3. Connect the other end of the cable to an available COM port of your computer.

Write down the COM port number you are using for the PassPoint system. You will need to know the COM port number when you configure your system.

## ***Step 6 - Mount and Connect the Keypad and Power Up the System***

The PassPoint system uses a standard ADEMCO 6139 alpha-numeric keypad (supplied with the ASK) to display system status and to annunciate trouble conditions such as door-open timeout alarms. The keypad can be mounted on the wall beside the main system cabinet or directly on the cabinet. Either way, the keypad should be mounted in an area where its display can be seen quickly and its audible signal can be heard. Only one keypad can be used with the PassPoint system.



---

The information provided in this section is only to get the system keypad up and running. Additional information about the keypad can be found in the installation instructions provided with the 6139 keypad.

---

### ***Keypad wiring and installation***

The keypad should be mounted on or near the cabinet only, and not wired through the premises. Use 22 AWG wire, to a maximum distance of 3 feet.

- 1. Remove the case back from the keypad by pushing down on the two snaps at the top of the case.**
- 2. Route wiring from the PassPoint control panel through the opening in the case back.**
- 3. Mount the case back to the wall or cabinet face.**



4. Plug the supplied flying lead connector into the keypad PC board.
5. Connect the wires of the keypad to the terminals of the PassPoint MLB as per the table below.

Keypad Wire	MLB Terminal
Red (+12VDC)	11
Black (Ground)	12
Green (Data In)	13
Yellow (Data Out)	14

6. Re-attach the keypad to its case back.

### ***Setting the keypad address***

The keypad's address must be set to "00" in order for it to function properly. If the address is not set correctly, an error message (Open Ckt) appears on the keypad display when the PassPoint system is powered up. To set the keypad address:

1. **Power up the PassPoint system.**

The keypad must be powered up in order to set the address.  
Powering up the PassPoint system powers up the keypad.

To power up the system, plug in the system's wallpack transformer.



Do not attempt to power up the system/keypad until previously described connections have been made.

---

2. **Within 60 seconds of power up, press and hold down the "1" and "3" keys of the keypad simultaneously.**

Pressing and holding down these keys puts the keypad into address mode. The current keypad address is shown on the display (“31,” the default address).

- 3. Press the “0” key twice to enter the new address, then press the star “\*” key.**

Pressing the star key saves the new address.

Once the proper address of “00” has been entered, the keypad will display the name of the system, the date, and the time (all of which are user-configurable).

## ***Step 7 - Connect the Optional 7 Ampere-Hour Battery***

If you have purchased the optional 12 volt, 7 ampere-hour battery, install the battery and connect it to the power supply as instructed below.



---

After battery installation, do not disconnect the system’s wall pack for any extended period of time. To do so will discharge the battery.

---

The battery should be mounted in the cabinet only.

- 1. Set the battery into the control panel case.**
- 2. Connect the black lead from the power supply BATT - terminal to the - terminal on the battery.**
- 3. Connect the red lead from the power supply BATT + terminal to the + terminal on the battery.**

## ***Where do you go from here?***

Now that all of your system hardware has been wired and mounted, you are ready to install the PassPoint *Plus* software. This software will enable you to configure and operate the PassPoint system.



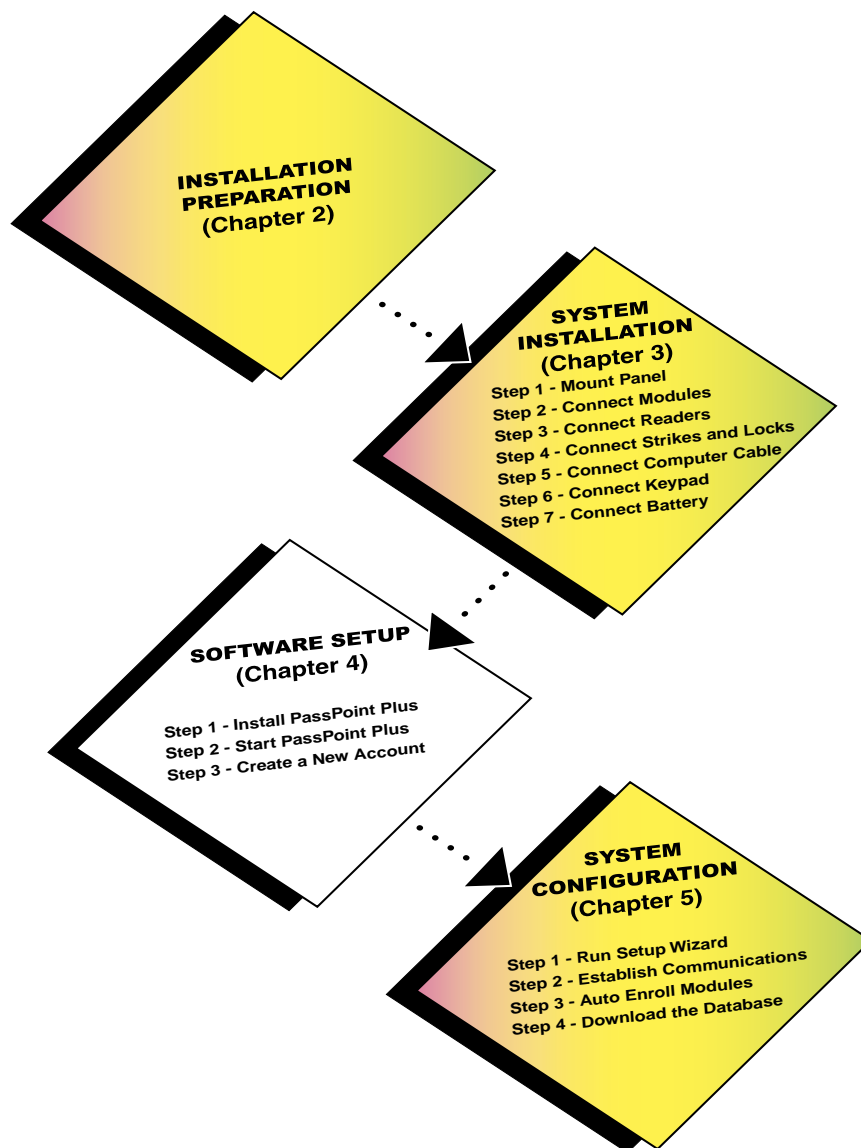
## Chapter

# 4

# *Software Setup*

This chapter explains the basic use of the PassPoint *Plus* Windows software program. In this chapter you will learn:

- **What PassPoint *Plus* is and what its system requirements are**
- **How to install PassPoint *Plus* on your user computer**
- **How to start PassPoint *Plus***
- **How to log on to PassPoint *Plus***
- **How to set up the communications parameters for PassPoint *Plus***



**STEP 1**  
**Install**  
**PassPoint**  
***Plus***

The first step in software setup is to install the PassPoint *Plus* software on your computer. Refer to the section of this chapter titled “*Step 1 - Install PassPoint Plus*” for instructions on performing this step.



**STEP 2**  
**Start**  
**PassPoint**  
***Plus***

Once the PassPoint software is installed, you can start it up. Refer to the section of this chapter titled “*Step 2 - Start PassPoint Plus*” for instructions on performing this step.



**STEP 3**  
**Create a**  
**New Account**

The first thing you must do after starting PassPoint *Plus* is set up your account. Each MLB in your system has one account. Accounts let you manage multiple MLBs. Refer to the section of this chapter titled “*Step 3 - Create a New Account*” for instructions on performing this step.

## ***What Is PassPoint Plus?***

PassPoint *Plus* is a Windows 95, Windows 98, and Windows NT 4.0-compatible software program that allows you to configure and operate the PassPoint access control system. Essentially, PassPoint *Plus* allows your computer to communicate with the main logic board of the system.

With PassPoint *Plus*, 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 *Plus* 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 *Plus* computer in order to function. The computer is primarily used to configure and monitor the system. Once the system is up and running, the computer can be disconnected (either intentionally or unintentionally) without disrupting the operation of the system. However, optionally configured event processing such as e-mail and/or pager event notification requires a fulltime connection to ensure timely delivery of the requested information.

---



## ***System Requirements***

In order to install and run PassPoint *Plus*, your computer must have the following minimum configuration:

### **Minimum**

- **Pentium-II® 200 MHz**
- **32 megabytes RAM**
- **80MB free hard disk space**
- **Windows 95, Windows 98, or Windows NT 4.0 (service Pack 3)**
- **SVGA video display, 800x600 resolution, 256 color**
- **Mouse**
- **Configured printer for reporting**

### **Recommended**

- **Pentium-III® 400 MHz or better**
- **64 megabytes RAM or better**
- **80MB free hard disk space or better**
- **Windows 95, Windows 98, or Windows NT 4.0 (service Pack 3)**
- **SVGA video display, 800x600 resolution, 256 color**
- **Mouse**
- **Configured printer for reporting**

### **Optional**

- **Sound Card, Modem, and Internet connection (for custom event handling)**
- **Integral Flashpoint Lite (or better) Video card for on-screen video support**
- **Twain-compliant image-input device, such as a digital camera and/or scanner, for cardholder imaging if desired**
- **Badge Printer for printing custom badges using the PassPoint Badger**
- **2 Hayes-compatible 28.8 modems (or better) used for PassPoint administration**

### **Display Setting Recommendations**

It is preferred that PassPoint Plus be used with an 800 X 600-display resolution with at least 16-bit color depth and a normal or small font setting.

### **Other System Issues**

The PassPoint *Plus* software will function properly with respect to basic features using the minimum required system. However, if you intend to use many of the optional features, such as custom event processing, or you intend to have a sizable configuration of hardware and/or cardholders, you will want to use at least the recommended system.

## Step 1 - Install PassPoint Plus

To install PassPoint *Plus* on your computer, follow the procedure below:

1. Close all programs that are running on your computer.
2. Insert the PassPoint CD into the computer. In a few moments, the first PassPoint screen will appear.

**NOTE:** If auto-start is disabled for your computer CD drive, click on the Windows *Start* button, click on *Run*, and then click the *Browse* button to find your CD drive. When you locate the CD drive, double-click on the CD drive and then double click on CDLaunch.exe. When the Run window reappears, click the *OK* button.

3. Position the cursor on *Install PassPoint Plus Software* and left-click the mouse.

In a few moments, the first screen of the PassPoint *Plus* installation program appears.

The PassPoint *Plus* installation program is designed to walk you step by step through the installation process. The program prompts you for the necessary information. Each time you complete a step, click *Next* to go on to the next step.

Once you have completed the installation process, the PassPoint *Plus* icon automatically appears on your desktop and *Start* menu.

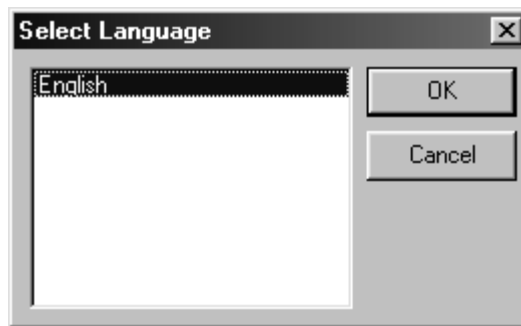


## ***Step 2 - Start PassPoint Plus***

To start PassPoint *Plus* on your computer:

**1. Select *PassPoint Plus* from the Windows Program menu.**

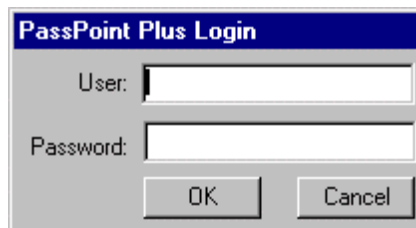
If this is the first time that PassPoint *Plus* has been started since it was installed on your computer, in a few moments the system will prompt you to select a language. This display will also be shown if on all previous starts of PassPoint *Plus*, *Cancel* was selected in response to the below prompt.



**NOTE:** English is the only language choice displayed in the above prompt at this time.

**2. Using the mouse, click *OK*.**

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



**3. Enter your default user name and password and click *OK*.**



Both the default User name and Password are *Installer*. Default logins exist for Installer, Master, Manager, and Operator; however, you need to log in as Installer in order to be able to do the complete installation. Once the system is operational, you should change the default logins for the system.

---

Once you click *OK*, the system brings up a new account dialog box. In order to continue, you must create a new account (see the next step in this chapter).

---



Always close PassPoint *Plus* before shutting down your Windows computer. Improper shutdown of your computer can cause the computer to experience shutdown problems, as well as possibly corrupting the PassPoint *Plus* database.

---

## Step 3 - Create a New Account

The first time you start PassPoint *Plus*, the system prompts you with a dialog box for creating a new Account:

The screenshot shows a 'Create New Account' dialog box with the following fields and options:

- Account Name: [Empty text box]
- Account Number: [Empty text box]
- MLE #: [Empty text box]
- Host ID #: [Text box containing 'FFFFFFFFFFFF']
- Port #: [Empty text box]
- Modem?:
  - ☒ No
  - ☐ Yes
- Modem Setup:
  - Phone #: [Empty text box]
  - Baud/Type: [Text box containing '52x128']
  - Buttons: [Empty], [Tone], [Pulse]
- ☒ Launch the Setup Wizard
- Buttons: [OK], [Cancel], [Help]

Before you can proceed to configuring your system, you *must* create a new account.

***What is an account?***

In order to make using your system's database efficient, PassPoint uses system *accounts*. An account is a *partition* of a database that allows *Plus* to manage more than one system (i.e., more than one 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 unique 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 *Plus* 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 *Plus*, you can select the account (i.e., site) you want to work with.

Even though your Starter Kit has only one MLB, you still need an account, because you cannot back up or restore the database without an account. In this case, you will need to set up only one account.

If the system is configured to dial into an alarm company central station, this account number will be used to identify all transmissions to the central station.

***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.

The first step is to create a new account for the one MLB included with your Access Starter Kit. To do so:

**1. Fill in the fields of the dialog box.**

The fields of the dialog box are described below:

**Account Name** - This is the name of the account for the MLB. You should provide the account with an easy-to-remember name that describes it properly. For example, if this is the account for the main MLB of the system, you might name the account "Main."

**Account Number** - This is the account number associated with the MLB account. This number can be up to four digits. Also, this number must correspond to the first four digits of the *Primary Subscriber Account Number* assigned to the MLB.

**MLB Number** - This is the number of the account's Main Logic Board, and is always 1.

**Host ID** - This is the host ID number for this account. The host ID is used to fill in the appropriate field on the network/ID tab of the screen of the system-wide options screen. The host ID is used to identify the correct computer host that is allowed to communicate with the MLB. When this value is at its initial value of FFFFFFFFFF, any computer host can communicate with the MLB.



It is essential that you remember the host ID number if it is changed. Without the changed number, the computer will not be able to communicate with the MLB.

---

**Port #** - Select the communications port of the computer to which you have connected the PassPoint system. This can typically be 1 through 8.



If your installation uses a LAN connection, enter 1 as the Port #. This will allow you to continue with the installation of PassPoint *Plus*. The LAN connection will be defined during System Configuration later in this manual.

---

**Modem?** - If you are using a modem to connect to the system, select *Yes*. If not, select *No*.

---



If your installation uses a modem, fill in the phone number at which your installed equipment can be reached. You may also need to modify the modem setup string if your modem requires special operational functions.

---

**Launch the Setup Wizard** - Click this box if you wish to launch the PassPoint *Plus* Setup Wizard to continue the account setup process when you select OK.

**2. Click *OK*.**

Clicking *OK* creates the new account. Once the account is created, the system presents you with the Setup Wizard if the Launch the Setup Wizard box was checked. The Setup Wizard is a tool for configuring your system.

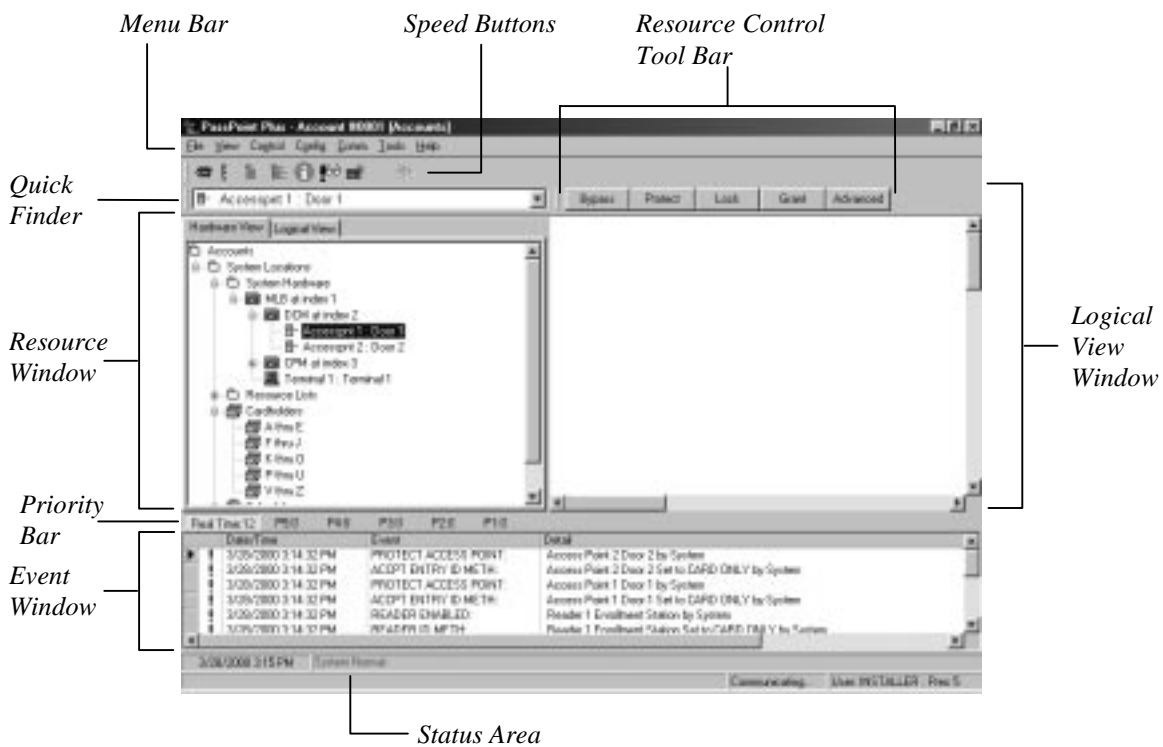
## ***The PassPoint Plus Environment***

PassPoint *Plus* is 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 *Plus* screen.



## Major screen components

The following illustration shows the main PassPoint *Plus* screen as it might look if the system were fully up and running. It includes cardholders, time schedules, etc.



The display shown above contains the default layout that is programmed into the PassPoint software. The content of the display and its arrangement may be changed by the installer or user.

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

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

**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.

**Priority Bar** - The priority bar allows you to select what is displayed in the Event Window. You may display a chronological listing of all events as they occur or a chronological listing of events for any one of the 5 priority levels.

**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.

**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 appears here in red.

**Logical View Window** - In the Logical View Window, floor plan(s) or 3-dimensional view(s) can be created showing the location of all of your system resources. Resources can be modules (like MLBs or DCMs), relays, zones, triggers, etc. Certain objects in the Logical View Window can be controlled by right-clicking on them.

**Resource Control Tool Bar** - The resource control tool bar contains buttons when you select certain items. These buttons

allow easy control of the selected item. For example, during operation, if you select an access point in the resource window, 5 buttons (Bypass, Protect, Lock, Grant, and Advanced) are displayed.

**Speed Buttons** - 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. If you are unsure of the function of a button, place the cursor over the button; a help bubble is displayed.



## Chapter

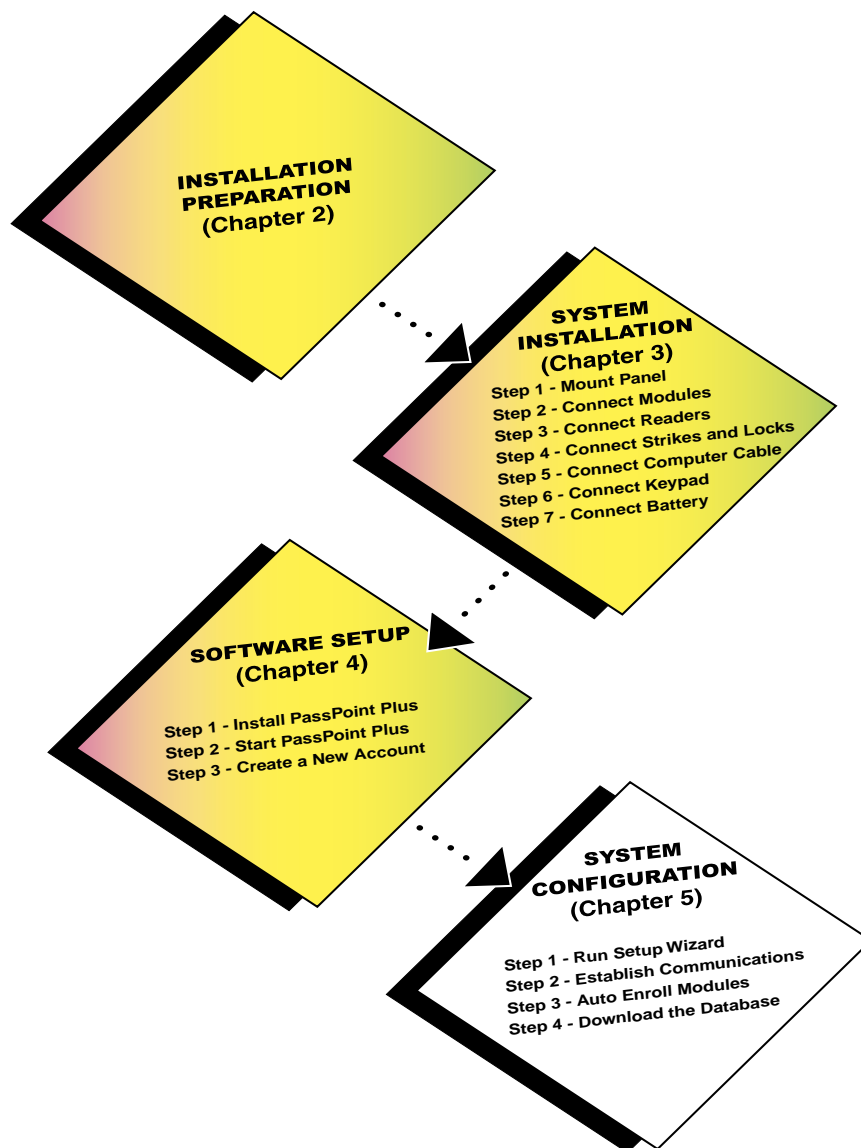
# 5

# *System Configuration*

This chapter explains the three main steps that need to be performed in order to get your PassPoint system up and running to a level that allows the first cards to be used.

In this chapter you will learn how to:

- **Set up your access points**
- **Enroll your system's Door Control Module**
- **Download the system database**
- **Enroll test cards and test the system**



**STEP 1**  
**Run the**  
**Setup Wizard**

The Setup Wizard is a tool that makes configuring your system as simple as possible. Refer to the section of this chapter titled “*Step 1 - Run the Setup Wizard*” for instructions on performing this step.



**STEP 2**  
**Establish**  
**Communications**

After running the Setup Wizard, you must connect to the MLB. Otherwise, PassPoint *Plus* will not be able to communicate with your PassPoint system. Refer to the section of this chapter titled “*Step 2 - Establish Communications*” for instructions on performing this step.



**STEP 3**  
**Auto Enroll**  
**Modules**

Whenever you add a new system module to your system, you must inform the system that the module is present. This is called enrolling. Refer to the section of this chapter titled “*Step 3 - Auto Enroll Modules*” for instructions on performing this step.



**STEP 4**  
**Download**  
**the Database**

Once you have enrolled your modules, you must download the information to the Main Logic Board, the main controller of the system. Refer to the section of this chapter titled “*Step 4 - Download the Database*” for instructions on performing this step.

## ***Step 1 - Run the Setup Wizard***

The first step in configuring your system is to run the Setup Wizard. The Wizard will help you to quickly set up your system by allowing you to choose from a predefined set of templates. Once you are done running the Wizard, your system will automatically have two doors, as well as a default access group, day template and schedule.

To use the Setup Wizard, simply follow the prompts on the screen. The first screen of the Wizard should already be on your screen:

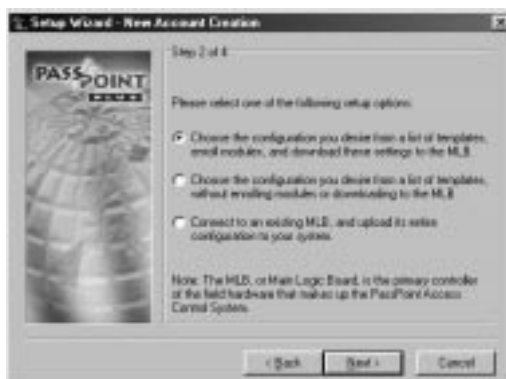


This is the introductory screen. It explains a little of what the Wizard will do for you.

### **1. Click *Next*.**

The second Wizard screen appears:

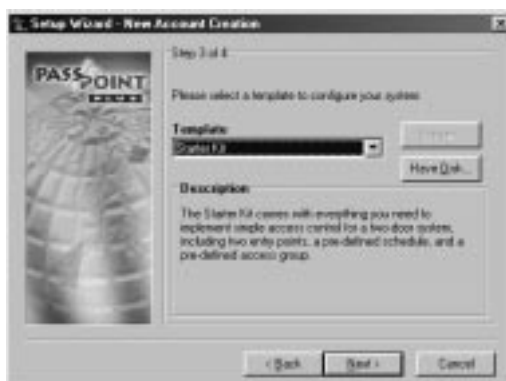




This screen presents you with three different setup options. The first option is the fullest option. It configures your system, enrolls your system modules, and downloads these settings to the database. Since you are setting up the system for the first time, this is the setup option to choose.

**2. Choose the first setup option, then click *Next*.**

The next screen of the Wizard appears:



This screen contains a drop-down list box that allows you to select a configuration template. By default, the system displays Starter Kit as the template to configure. If you are only configuring a Starter Kit without an Expansion Kit or

Card Enrollment Kit, select this option. Otherwise, select the appropriate option from the list. For the purposes of this discussion, we will assume you are only configuring a Starter Kit.

**3. Select a template, then click *Next*.**

If you have chosen the Starter Kit template, the final screen of the Wizard appears:



Click *Finish* in this screen to finish your configuration. The system will automatically create your two access points (i.e., doors), and create a default access group, day template and schedule. You will learn how to use each of these items in later chapters of this guide.

Once the new account is configured, the system prompts you to connect to the MLB so that you can enroll your modules and download the new configuration.

## Step 2 - Establish Communications

After running the Setup Wizard, you must connect to the MLB. Otherwise, PassPoint *Plus* will not be able to communicate with your PassPoint system.

Before setting up PassPoint *Plus*, make sure you have connected your PassPoint system to your computer via a direct wire or modem connection. For a direct wire connection, a null modem cable has been provided for connecting the RS-232 connector of your MLB to one of the COM ports of your computer.

Power up the panel and wait for the keypad to display the message “LOCAL ONLINE.” If you are using a modem at the panel, press and release \* and # simultaneously, then wait for the keypad to display the message “REMOTE OFFLINE.”

The Connect to MLB dialog box appears immediately after running the Setup Wizard:



This dialog box displays information about your MLB connection parameters.

1. **Perform either step “a” (direct or modem connection) or “b” (LAN connection) below.**

- a. Click *Connect*.
- b. Click on the *Setup* button. A communications setup dialog box is displayed.



In the dialog box, select LAN, enter your IP address in the LAN Name/IP box, click *Update*, and then click *Close*. The MLB connection dialog box reappears.

Click *Connect*.

After a few moments, the *Connected* field will change from “False” to “True,” indicating that connection has been established between your computer and your system’s MLB.

If you have chosen a modem connection, the modem connected to the computer will dial the appropriate phone number in order to reach the “remote” MLB.

2. Click *Close* in the *Connect to MLB* dialog box if it is still being displayed. In most first-time installations, the *Connect to MLB* dialog box cleared when *Connect* was selected above.

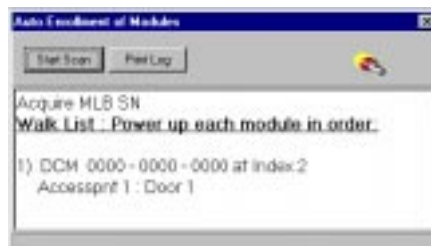
The MLB has now established a connection with the computer.

## Step 3 - Auto Enroll Modules

After connecting to the MLB, the system automatically prompts you to enroll your modules. Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system goes out and searches for any modules connected to it that have not been enrolled. Your kit template defines the hardware modules that the system expects to find. It knows which modules are not enrolled because these modules have serial numbers that contain all zeros. For instance, look at the DCM you have just added with the Wizard. It has a serial number that contains only zeros. That means that it has not been enrolled, and that it is not truly part of the system yet.

The Auto Enroll dialog box should already be on your screen, and should look something like this:



As you can see, the dialog box contains instructions. First, the system acquires the serial number for the MLB. Then it scans for the DCM and enrolls that serial number as well.

This is all done **automatically** once you click *Start Scan*. The entire process will not take more than a few moments. The system knows which modules to look for because of the Starter Kit

template you chose using the Setup Wizard. If you had chosen a different template, say a Starter Kit with a Card Expansion Kit, the system would also scan for a CPM. The procedures required to enroll a single module are different than those required to enroll multiple modules. If enrolling a single module, refer to the *Enrolling a Single Module* paragraph below. If enrolling more than one module, refer to the *Enrolling Multiple Modules* paragraph below.

## ***Enrolling a Single Module***

To enroll a single module into your PassPoint system, proceed as follows:

---



Never power down the MLB while the system is enrolling a module.

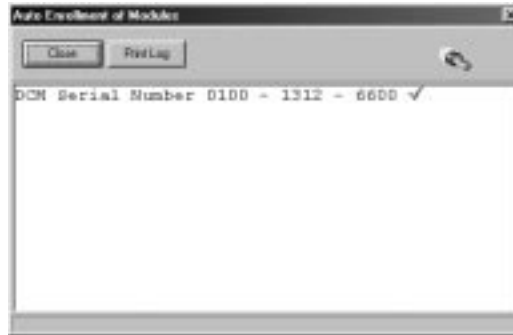
---



### **1. Click the *Start Scan* button.**

The system searches for the module. When the module is found, the system blinks the yellow service LED on the module, presents a screen message indicating that the module has been enrolled, and stops scanning for modules.

After the system has enrolled the module, a screen is presented that shows the module (with serial number) that has been enrolled.



**2. Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

## ***Enrolling Multiple Modules***

The Auto Enroll dialog box should already be on your screen, and should look something like this when enrolling multiple modules:




If the modules are powered up before the enrollment process or powered up in the wrong order, they will be enrolled incorrectly. Never power down the MLB during the enrollment process.

To enroll multiple modules into your PassPoint system, the modules must be powered up in the order that they are listed on the screen. To enroll the modules, proceed as follows:

A rectangular button with a grey gradient and a black border, containing the text "Print Log" in a black sans-serif font.

1. **Click the *Print Log* button.** A “walk list” of all the modules waiting to be enrolled is printed.
2. **Verify the power is applied to the first module listed only.**

**NOTE:** You must power up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered up.

A rectangular button with a grey gradient and a black border, containing the text "Start Scan" in a black sans-serif font.

3. **Click the *Start Scan* button.**

The system searches for the first module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. Next, a message will be displayed indicating that the system is polling for the next module in the “walk list.”

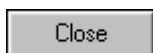
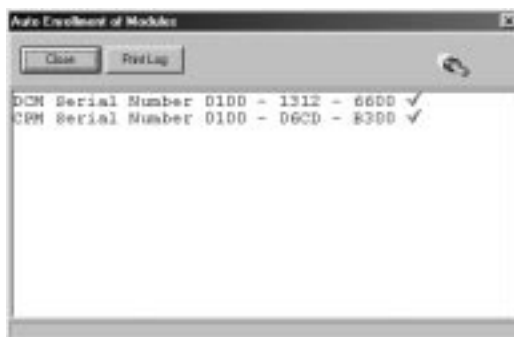
4. **Apply power to the next module in the list.**

The system searches for the next module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. If additional modules are in the list, a message will be displayed indicating that the system is polling for the next module.”

5. **Repeat the application of power to the modules, one at a time, until all modules have been enrolled.**



When the system has enrolled the last module in the list, the screen shows a listing of modules (with serial numbers) that have been enrolled.



**6. Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

## ***Step 4 - Download the Database***

The last step to getting your system operational is to download the database.

A copy of the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your computer, these changes are not automatically made to the database on the MLB. They are kept in your computer until you download them to your MLB database. Any changes made on the computer must be downloaded to the database in order for them to take effect.

*For example, you have already added a DCM to the system. The DCM has one or two doors that you have configured. This information is all displayed in the PassPoint Plus window. It resides in the computer database. But it does not yet reside in the primary MLB database, because you have not downloaded it yet.*

To download the database, follow the procedure below:

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

The Download dialog box appears:

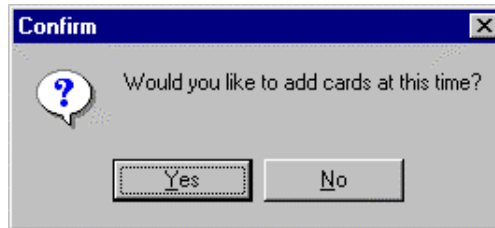


At the top of the dialog box is the account number you will be downloading. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes are automatically checked according to the kit template you have selected.

**2. Click *Start*.**

The database download proceeds. The status bar at the bottom of the dialog box tracks the progress of the download.

When download is complete, a dialog box appears asking if you want to add cards.



Clicking *Yes* automatically launches the Card Wizard, a PassPoint tool used for quickly adding cards to the system. Adding cards to the system is covered fully in the next chapter of this guide.



## Chapter

# 6

# *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**
- **Bulk edit cards**
- **Use the Card Monitor**

## 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 code, 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, and 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 work for only three entries into your building, you can set the card to deny every entry request after the third.*

**Where do you start?**

In Chapter 5, you configured your system and were prompted to add cards. Essentially, adding cards is the last step in the setup process. The system prompted you with the Card Wizard, as shown below:



You can also call up the Card Wizard by clicking the Add Card button on the button bar.

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 at a time. 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 allows you to add only 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:

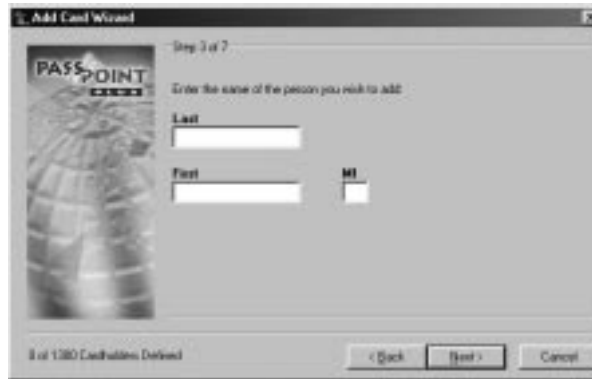


### ***Adding a single card***

To enter a single card using the Card Wizard:

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

The Wizard asks you to enter a last name, first name, and middle initial 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 prompts 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 field manually.



The default card setting is 34-bit ADEMC0 proximity.

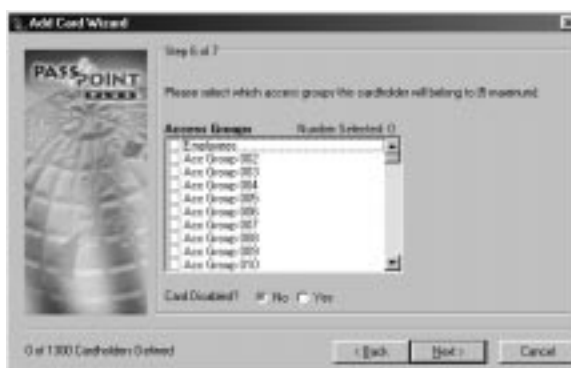
### 3. Enter the card information and click *Next*.

The Wizard asks you to enter a PIN number for the card. This is an optional step and needs to be done only 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 asks you to choose access groups for the card:



Each cardholder can be assigned to up to 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 at its default value of 0 (zero).

**6. Click *Finish*.**

The card is 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 asks 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 automatically enrolls 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.

Once the cards have been swiped, you then choose an access group for the cards. Also, this method gives you an option of entering a cardholder name for each card you enroll.

## ***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, as 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* or click on the *Add New Card* speed button.

The Confirm dialog box appears:



2. To add cards manually, click on *NO*.

The Card Data dialog box appears:

Each tab allows you to add, edit, or view different data for the card.

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

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 a unique *Card Code* and/or *PIN Code* are mandatory while some others, like *Last Name* and *Access Groups*, are recommended. 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.

### 3. 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 reads “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 unless the card technology being used is raw card image data, which is not normally used. 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 in 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).

**Disabled** - If you want to disable the privileges of the cardholder, check this box. While disabled, all of the cardholder's access privileges are revoked. You can reinstate the cardholder's privileges at any time by unchecking this box. While disabled, the card remains 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.

**Denial CAL and Additional CAL** - These fields are for future use and are not active in this version of *PassPoint Plus*.

**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 are not checked, so it is not strictly necessary to assign any access groups (although it is highly advisable, as 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 has 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 is not used unless a card needs to be “watched” for some reason.

**4. 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 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.*

**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 is the name assigned to that relay when it was configured.

**NOTE:** Resources must be defined and configured before you are allowed to assign them in the Specifier field.

**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 is not allowed to occur. The default value for this field is 0, meaning normal.

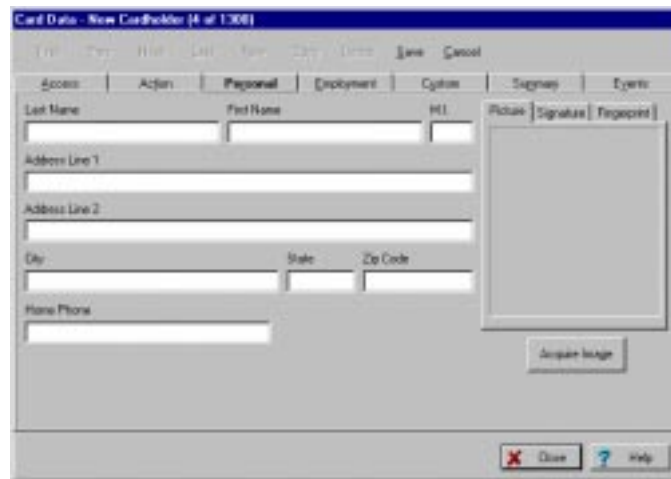
**Precedence Change** - This field indicates how the precedence level of the Specifier (above) will be affected when the action takes place. You can choose None, Clear the precedence level to 0, or Update to have the resource take on the precedence level of the cardholder.

**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 (not configured as part of an access point) command reader.

## ***Using the Personal tab***

You can enter personal information about a cardholder into the cardholder database. To do so, use the fields of the Personal tab:

The screenshot shows a software window titled "Card Data - New Cardholder (4 of 100)". It features a tabbed interface with tabs for "Access", "Action", "Personal", "Employment", "Custom", "Signature", and "Events". The "Personal" tab is currently selected. It contains several input fields: "Last Name", "First Name", and "M.I." at the top; "Address Line 1" and "Address Line 2" in the middle; "City", "State", and "Zip Code" below that; and "Home Phone" at the bottom left. On the right side of the "Personal" tab, there are three sub-tabs: "Picture", "Signature", and "Fingerprint". Below these sub-tabs is a large rectangular area for image acquisition and an "Acquire Image" button. At the bottom right of the window are "Close" and "Help" buttons.

**Last Name, First Name, M.I.** - These fields are duplicates of the fields found on the Access tab and are placed here for user convenience.

**Address Line 1, Address Line 2, City, State, Zip Code, and Home Phone** - The cardholder address and phone number can be stored in these fields.

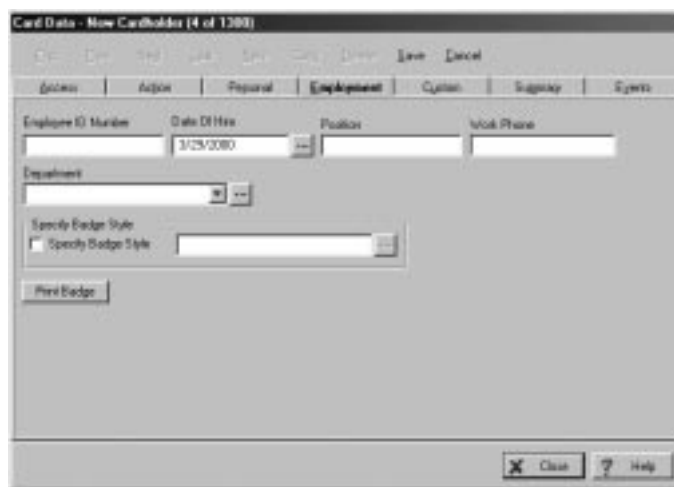
**Acquire Image (Picture, Signature, and Fingerprint)** -The tabs in Acquire Image are used to store various bit-mapped images for the cardholder. These images can be acquired by using the Acquire Image button. The Acquire Image button allows the user to import an image from any TWAIN-compliant image source, or import an image from a disk file. A disk file image can be in any one of several graphic file formats including Bitmap, JPEG, and GIF. The

Signature tab may be used in conjunction with most Windows-compatible writing tablets to capture a cardholder signature.

Note that, when the cardholder's picture is included in the database, the Card Monitor feature (described later in this chapter) can be used to view a cardholder's picture on cardholder initiated events.

## Using the Employment tab

The cardholder database can also retain cardholder employee identification data. To enter cardholder employee identification data into the cardholder database, use the fields of the Employment tab:

The screenshot shows a Windows-style dialog box titled "Card Data - New Cardholder (4 of 1300)". It has a standard menu bar (File, Edit, View, Tools, Options, Window, Help) and a toolbar with buttons for Save and Cancel. Below the toolbar is a tabbed interface with tabs for Access, Action, Personal, Employment (which is selected), Custom, Signature, and System. The Employment tab contains several input fields: "Employee ID Number" (a text box), "Date Of Hire" (a date picker showing 3/23/2080), "Position" (a text box), and "Work Phone" (a text box). Below these is a "Department" dropdown menu. Further down is a "Security Badge Style" section with a checkbox labeled "Specify Badge Style" and an associated dropdown menu. At the bottom left of the tab is a "Print Badge" button. At the bottom right of the dialog box are "Close" and "Help" buttons.

**Employee ID Number** - This field is used to record the cardholder employee ID number.

**Date Of Hire** - This field is used to record the date the cardholder was hired. Valid dates range between January 1, 1950 through December 31, 3999. Clicking the button to the right of the Date Of Hire field will make a calendar be displayed.

**Position** - This field is used to record the cardholder's position/job title.

**Work Phone** - This field is used to record the cardholder's work phone number.

**Department** - This field is used to record the department that the cardholder works in. You can select from a list of departments already defined by clicking the down arrow at the right of the field. You can also create a new department by clicking on the button to the right of the field. When you click on the button, a Department / Badge Styles screen will be displayed where departments can be added or deleted and badge styles selected.

**Specify Badge Style and Print Badge** - This field and button are used to specify a badge style and print a badge if you are using the PassPoint Badger and have already created at least one master badge file.

## ***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 the fields have not been configured yet except, field 6. By default, field 6 holds the card number data.



To configure fields for the *Custom* tab:

1. From the *Config* menu, select *Cards>Custom Fields*.

The Cardholder Custom Fields 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.



---

Custom Field 6 is reserved for use by the PassPoint *Plus* Program. It can not be edited or changed.

---

**Enable Field** - This allows 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.

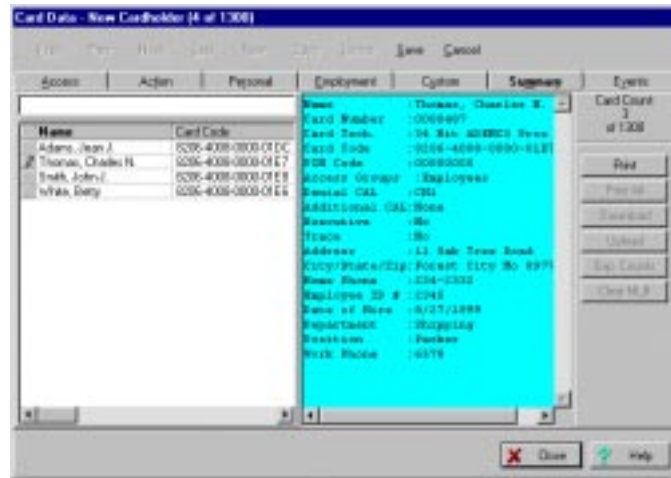
**3. Click *OK*.**

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.

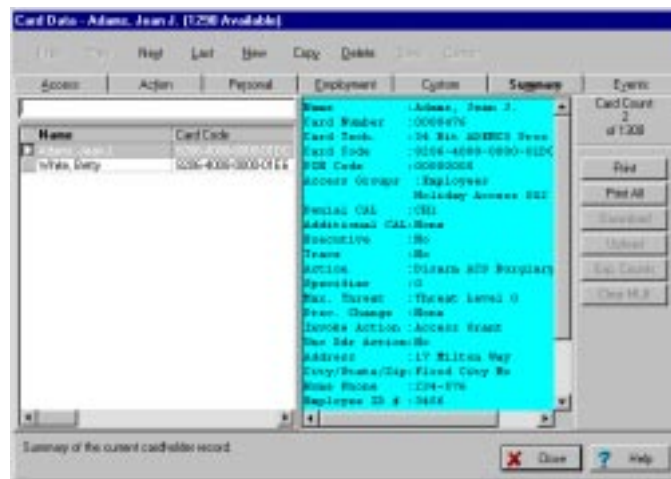
## ***Using the Summary tab***

The Summary tab displays a summary of all identification information that has been recorded about a cardholder. When you are storing data for a new cardholder, the pencil symbol to the left of the name denotes the cardholder whose summary information is displayed. When defining a new cardholder, if you right-click on the pencil symbol, a sub-menu appears asking if you wish to save or cancel the modified cardholder information.





When the cardholder summary is accessed during a Cards/Browse database selection, the Cardholder screen takes on a slightly different appearance and functions differently. This screen is shown below:



The following functions are available when you are using the Cards/Browse database selection:

1. Left-clicking on a column head sorts the cards into order for that column head. For example, left-clicking on the column head for Name puts the cards into name order. (Note: Changing the sort of this list also changes the order of the card database as it pertains to the navigation buttons at the top of the form).
2. If you right-click in the area containing the list of cardholders, a list of options appears for resorting the list into name, card code, pin code, ID number, or card number order.
3. Once you have sorted cardholders according to the desired field, you may search by beginning to type the desired information in the Search Edit box above the list of cardholders. As you type, the information is automatically completed for you as the system finds the nearest matching record. If you select a sort according to the Card Code, and are on-line with the MLB, you may swipe the card at any enrollment reader, once the input focus (cursor) is in the Search Edit box. The system searches the card database for the card swiped. If it is found, that card will be highlighted in the list. Otherwise, an on-screen message appears stating that the card was not found.
4. The arrow to the left of the name indicates which cardholder the summary is displaying information about.
5. All command buttons on the right side of the screen become active when the computer is connected to an MLB. When not connect to the MLB, only the Print and Print All buttons are active. The buttons provide the following functions:

**Print** - This button prints the summary information about the selected cardholder.

**Print All** - This button prints the summary information about all cardholders.

**Download** - This button downloads any changes in the card database to MLB. This button needs to be used only if the card database was modified while off-line.

**Upload** - This button clears the cardholder database from the computer and uploads the cardholder database from the MLB into the computer.



---

**CAUTION:** The Upload button should be used only in extreme conditions and with extreme caution, as it erases all non-access related cardholder information (address, custom fields, etc.).

---

**Exp. Counts** - This button traverses the entire card database in the MLB and uploads the expiration usage counts for any cards that use them.

**Clear MLB** - This button requests that the MLB default its copy of the card database and then asks you to re-create all of the card records on the MLB by downloading the cardholder database from the computer.



---

**CAUTION:** The Clear MLB button should be used only in extreme conditions, as you are attempting to restore the functionality of a defaulted MLB.

---

## ***Using the Events tab***

The PassPoint system can display events by cardholder over a selected period of time. To obtain this function, select the Events tab. The following screen appears:



To select a time period to display events for, position the cursor on the “from” date field and click the mouse. A dialog box appears asking you to select a starting date. Select the starting date. Then position the cursor on the end date field and click the mouse. A dialog box appears asking you to select an end date. Select the end date.

Events that have occurred for the selected cardholder during the selected period are displayed.

Note that on a new cardholder, the events log will be empty unless you are re-assigning a card that was previously deleted. If you are re-assigning a card, if any prior activity occurred during the selected time period, these activities are displayed.

## ***Bulk Editing Cards***

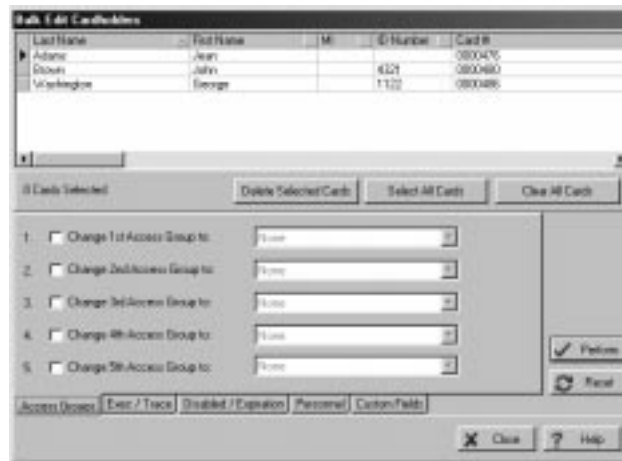
The PassPoint program allows you to edit cards in bulk. This feature is normally used to change the content of a field in the

cardholder database for several cardholders at the same time. When you use this feature, you do not have to repeatedly call individual cardholder records and make redundant changes.

To bulk edit cards, follow the procedure below:

**1. From the Config menu, select Cards>Bulk Edit Cards.**

The Bulk Edit Cardholders dialog box appears:



The dialog box contains several items that are common to each tab in the Bulk Edit Cards dialog. These items are:

**Cardholder Selection Area** – This area of the screen contains cardholder names, ID numbers, card numbers, personal data, access groups, and privileges. You can select multiple cardholders by using SHIFT-click and CONTROL-click mechanisms standard to Windows™ or you can left-click and drag up or down anywhere in the data area to select contiguous cardholder records. You can also use the Select All Cards or Clear All Cards buttons to set your selection of cardholders appropriately (see below).

The presentation of this data in this area can be modified as follows:

- The order that cardholders are listed can be modified by clicking on the arrow at the top of each column. The sort order choices are ascending (first click), descending (second click), or none (default or third click). Note that the system ranks columns for precedence when it comes to sorting: Sorting is prevented on any column to the right of the first column a user selects from the left side of the screen.
- The order that columns are presented can be reorganized by clicking in the column heading to select the column, and then depressing and holding the mouse button while dragging the column to the location desired.

**Delete Selected Cards** – When you click this button, the system asks you to confirm the deletion of the selected cards. If you answer “Yes,” the card is either deleted or marked for deletion, depending on the status of that cardholder record, and is removed from the viewable list of cardholders.

**Select All Cards** – Click this button to select every cardholder in the selection grid.

**Clear All Cards** – Click this button to deselect every cardholder in the selection grid.

**Perform** – Click this button to insert into the cardholder data, any changes you have made on the current screen. At the end of the modification process, you are told exactly how many card records were modified. This number may not be the same as the number of cardholders that were selected. This is because if the data for a selected cardholder already matches the settings you wish to change to, then the cardholder record is not modified. If you have made changes to the current screen and select a different Bulk Edit Cards tab without clicking the Perform button, the system presents a message asking if you want to perform the changes before leaving. At that screen you can elect to perform the changes by answering *Yes*; to delete

the changes by answering *No*; or to remain on the current tab by answering *Cancel*.

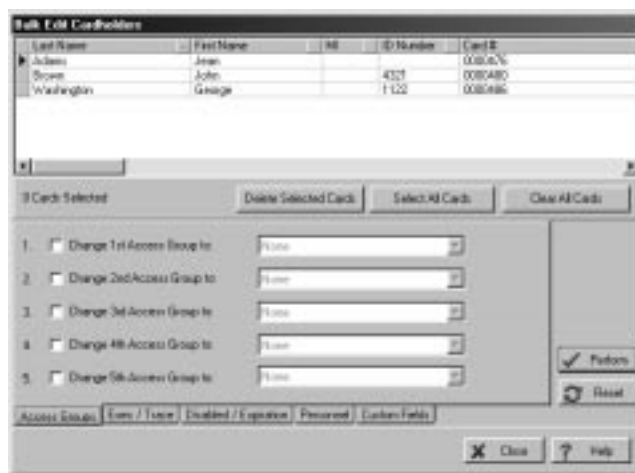
**Reset** – Click this button to discard any changes you have made on the current screen.

**Close** – Click this button when all changes have been made. The screen is cleared and the changes downloaded to the MLB.

**Help** – Click this button to display the Bulk Edit Cards help screen.

## Bulk editing cardholder access group assignments

When Cards>Bulk Editing is selected from the Config menu, the Bulk Edit Cardholders dialog box appears:



To change access group assignments for cardholders, observe the following procedure:

1. **Select the cardholders desired for an access group assignment change using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

2. **Select the Access Group to be changed (1 through 5) by clicking on the corresponding box.**
3. **Click the down-arrow to the right of the access group being changed and select a new group from the list presented.**
4. **Click on the Perform button. The changes are inserted into the cardholder data.**
5. **Repeat steps 2 and 4 for each access group being changed.**

## ***Bulk editing cardholder executive privileges/trace***

To bulk edit cardholder executive privileges and trace assignments, click on the Exec/Trace tab. The Bulk Edit Cardholders executive privileges/trace dialog box appears:

**Bulk Edit Cardholders**

Last Name	First Name	ID	ID Number	Card #
Adams	John			0000476
Brown	John		4101	0000480
Washington	George		1122	0000486

8 Cards Selected

☐ Change Executive Privileges Option to:

☐ Change Card Trace Option to:



To change executive privileges/trace assignments for cardholders, observe the following procedure:

1. **Select the cardholders desired for an access group assignment change using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

2. **Select the access group to be changed (1 through 5) by clicking on the corresponding box.**
3. **Click the down-arrow to the right of the access group being changed and select a new group from the list presented.**
4. **Click on the Perform button. The changes are inserted into the cardholder data.**

### ***Bulk editing cardholder disabled/expiration data***

To bulk edit cardholder disabled and expiration data, click on the Disabled/Expiration tab. The Bulk Edit Cardholders disabled/expiration dialog box appears:

Last Name	First Name	ID	ID Number	Card #
Adams	John		4201	0000470
Brown	John			0000480
Washington	George		1122	0000486

To change the disabled/expiration data for cardholders, observe the following procedure:

**1. To change the Disabled flag for some cardholders, proceed as follows:**

- a. **Select the cardholders desired using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

- b. **Select “Change Disabled Flag to:” by clicking on the corresponding box.**
- c. **Click the down-arrow to the right of the selected option and select No or Yes from the list presented.**
- d. **Click on the Perform button. The changes are inserted into the cardholder data.**

**2. To change the Expiration Date Setting for some cardholders, proceed as follows:**

- a. Select the cardholders desired using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

- b. Select “Change Expiration Date Setting to:” by clicking on the corresponding box. The Use Expiration Date field becomes active.**
- c. Click the Use Expiration Date box. The calendar field to the right of the box becomes active.**
- d. Enter a date in the calendar field. The date can be entered from the keyboard or you may click on the button to the right of the calendar field and select a date from the calendar displayed.**
- e. Click on the Perform button. The changes are inserted into the cardholder data.**

**3. To change the Expiration Count Setting for some cardholders, proceed as follows:**

- a. Select the cardholders desired using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

- b. Select “Change Expiration Count Setting to:” by clicking on the corresponding box. The Use Expiration Count field becomes active.
- c. Click the Use Expiration Count box. The count field to the right of the box becomes active.
- d. Enter a count in the count field. The count can be entered from the keyboard or you may click on the button to the right of the count field until the desired number is displayed. Valid entries are from 1 to 65,534.
- e. Click on the Perform button. The changes are inserted into the cardholder data.

## ***Bulk editing cardholder custom fields***

To bulk edit cardholder custom field data, click on the Custom Fields tab. The Bulk Edit Cardholders custom fields dialog box appears:

Last Name	First Name	MI	ID Number	Card #
Adams	John	4	4321	0000470
Brown	John	4	4321	0000480
Washington	George	1	1122	0000486

8 Cards Selected    Delete Selected Cards    Select All Cards    Clear All Cards

☐ Change Custom Field 1 to:   
☐ Change Custom Field 2 to:   
☐ Change Custom Field 3 to:   
☐ Change Custom Field 4 to:   
☐ Change Custom Field 5 to:

Perform    Reset

Access Groups    Exec / Trace    Disabled / Expiration    Personal    Custom Fields

Close    Help

To change the custom fields data for cardholders, observe the following procedure:

**NOTE:** If a custom field or fields have not been defined in your system, the fields on this screen are not active.

1. **Select the cardholders desired for a custom field change using one of three methods: press the Select All Cards button; Shift-Click on the cardholders; or Ctrl-Click on the cardholders.**

Note that if it makes your selection easier, the order in which the cardholders appear can be changed using the sort features previously described.

2. **Select the Custom Field to be changed (1 through 5) by clicking on the corresponding box.**
3. **Type the new custom field information in the custom field box to the right of the selected “Change Custom Field to:.”**
4. **Click on the Perform button. The changes are inserted into the cardholder data.**
5. **Repeat steps 2 and 4 for each custom field to be changed.**

## ***The Card Monitor***

The PassPoint *Plus* program allows you to view a cardholder’s picture on your computer screen when the cardholder causes an event to appear in the event log (i.e., access grant). To use this feature, the cardholder’s picture must be part of the “*Personal*” record in the cardholder database and the PassPoint Plus computer must be connected to the MLB. Procedures are provided below for creating a Tool to call the Card Monitor and for Using the Card monitor.

## ***Creating the Card Monitor Tool***

The Card Monitor can be started by adding it as a tool in PassPoint *Plus*. To add the Card Monitor to the Tools menu, proceed as follows:

- 1. Click on the *Tools* tab at the top of the PassPoint *Plus* screen.**
- 2. Click on *Configure Tools* in the drop-down menu.** A Configure Tools screen is displayed.
- 3. Click on the *Add* button.** A Tools Properties screen is displayed.
- 4. In the *Title* area of the Tools Properties screen, type “Card Monitor.”**
- 5. Position the cursor in the Program area of the Tools Property screen and click on the *Browse* button.** The PassPoint *Plus* file directory is displayed.
- 6. Scroll through the PassPoint *Plus* file directory until you reach “CardActMon.exe” and double-click on it.** The file is added to the Program area of the screen and the Working dir area of the screen is automatically filled in.
- 7. Click on the *OK* button in the Tools Properties screen.** The screen closes and the Card Monitor is added to the Configure Tools screen.
- 8. Click the *Close* button on the Configure Tools screen.** The Card Monitor is now an available tool for PassPoint *Plus*.

## Using the Card Monitor

The Card Monitor is started by selecting it from the Tools menu in PassPoint *Plus*. To use the Card Monitor, proceed as follows:

**NOTE:** Your computer must be on-line (connected) with the MLB and the cardholders' pictures must be in their Personal record in the cardholders database for this feature to operate properly.

1. Click on the **Tools** tab at the top of the PassPoint *Plus* screen.
2. Click on **Card Monitor** in the drop-down menu. The Card Monitor is now running and a card monitor window is added to your screen. The card monitor window appears as follows:



When an event occurs (i.e., access grant), the cardholder's picture is displayed in the Card Monitor window as shown below:



Event information can be obtained using the Card Monitor window, or the Card Monitor can be moved, minimized, or exited as detailed below:

*Obtaining Cardholder Event Information* – Position the cursor in the picture area of the Card Monitor window and left-click the mouse. Information about the event that triggered the cardholder's picture display is presented. The information will appear as shown in the example below:



*Moving the Card Monitor window* – The Card Monitor window can be moved in either of two ways as detailed in **a.** and **b.** below:

- a.** Position the cursor on the bar at the top of the Card Monitor window, hold down the left mouse button, and drag the window to the position desired.
- b.** Position the cursor on the bar at the top of the Card Monitor window and right-click. A popup menu appears. Select *Move* from the popup menu and the Card Monitor window can be moved using your arrow keys on the computer keyboard to move the window or holding down the left mouse button and dragging the window.

*Minimizing the Card Monitor window* – The Card Monitor window can be minimized in three ways as detailed in **a.**, **b.**, and **c.** below:

- a.** Position the cursor on the X at the top-right corner of the Card Monitor window and left-click the mouse.
- b.** Position the cursor in the picture area of the Card Monitor window and right-click. A popup menu appears. Select *Minimize* from the popup menu and the Card Monitor window is minimized.



- c. Position the cursor on the bar at the top of the Card Monitor window and right-click. A popup menu appears. Select *Close* from the popup menu and the Card Monitor window is minimized.

*Exiting the Card Monitor* – The Card Monitor can be exited by right-clicking in the picture area of the Card Monitor window. A popup menu appears. Select *Exit* from the popup menu and the Card Monitor is exited and removed from the screen.



## Chapter

# 7

# *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.

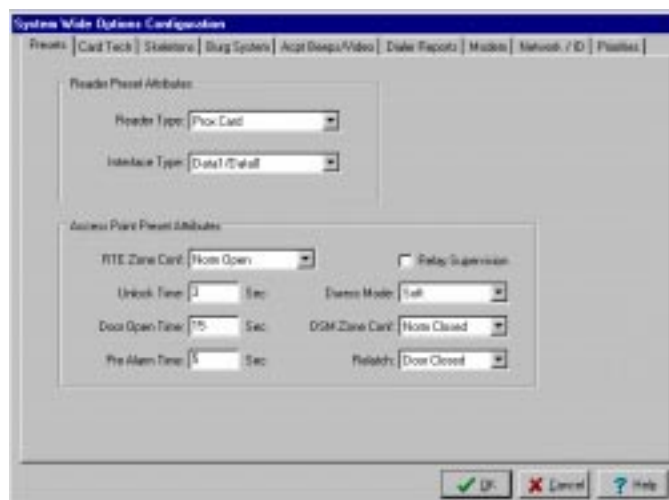
System-wide options include:

- **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 or from the Config menu:

*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. Detailed descriptions of each field are provided in the following paragraphs.

When you are finished 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, as these settings will automatically be invoked for you when you add hardware to the system.



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

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

The reader preset attributes entered in the following fields will be automatically filled in for you when you assign readers to the system; however, you can override them by selecting different settings when you configure the individual hardware modules.

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

**Interface Type** - In this field, select the electrical interface to be used by your readers.

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

The access point preset attributes entered in the following fields will be automatically filled in for you when you configure access points in the system; however, you can override them by selecting different attributes when you configure the individual access points.

**RTE Zone Conf** - Select the zone configuration that will be used for RTE zones.

**Unlock Time** - Enter the default unlock time (in seconds) for access points.

**Door Open Time** - Enter the default door open time (in seconds) for access points.

**Pre-Alarm Time** - Enter the default pre-alarm time (in seconds) for 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..

**Duress** - In this field, choose the duress mode setting for access points.

**DSM Zone Conf** - Select the zone configuration that will be used for DSM zones.

**Relatch** - In this field, choose the relatch option for access point door control relays.

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

## ***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-Wide Options Configuration' window with the 'Card Tech' tab selected. The 'Card Recognizers' table lists four entries: 1. ACC Wiegand 26, 2. ACC Ademco Wiegand 34, 3. ACC Omnicast-DHPIA 34, and 4. Bit Image of Specified Length. Below the table, the 'Card Lengths' section contains four input fields: 'Wiegand Card Bits' set to 26, 'Proximity Card Bits' set to 34, 'Magnetic Strip Card Bits' set to 26, and 'Proximity PPS Digits' set to 4. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Num	Name	Field A	Field B	Field C
1	ACC Wiegand 26	0	0	256
2	ACC Ademco Wiegand 34	0	0	256
3	ACC Omnicast-DHPIA 34	0	0	0
4	Bit Image of Specified Length	0	0	0

Card Lengths:

Wiegand Card Bits: 26  
Proximity Card Bits: 34  
Magnetic Strip Card Bits: 26  
Proximity PPS Digits: 4

### ***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 that 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 that 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. Setting this length to 254 will strip off the parity bits from each American Banking Association (ABA) character and simplify identification of raw card data. Setting the length to 254 also enables the *Config Mag* button. Selecting the *Config Mag* button provides a screen where the format of the magnetic strip card can be edited. See the ABA Mag Strip Configuration paragraphs below for a description of the ABA Mag Strip Configuration screen.

**Keypad PIN Length** - This field can be set from three Personal Identification Number (PIN) digits to eight digits. 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. This

means that if you use 4 PIN digits, the first THREE digits of every PIN number assigned in the system MUST be unique.

## ***ABA MagStripe Configuration screen***

To access the ABA MagStripe Configuration screen, change the Magnetic Stripe Card Bits value to 254 and select the Config Mag button on the System Wide Options, Card Tech tab. The configuration screen below appears:

The following paragraphs define the functions of each of the fields and incorporate a discussion of the ABA Track 2 requirements.

## **FORMAT TABS**

There are four tabs in the upper left-hand corner of the screen. These tabs are used to select which of the four ABA formats you wish to modify. The default formats are:

**Format C**, Kronos Format – This format can be used to recognize Kronos cards from an existing time and attendance system. If the

“Time Keeping System’s ACM” type bar code readers are used (configured to output ABA format), this stock format should work for you as it exists.

**Format D** – An example of an ABA format.

**Format E** – Another example of an ABA format.

**Format F** – An example of a credit card format. In some cases, a credit card can be used for access control. Be careful, as many cardholders do not wish to have their credit card number enrolled in an access control system.

## **NAME**

The Name field simply helps you identify a particular format. These names should be kept as descriptive as possible. If it will describe your company’s encoded format, you might give it a name like “ABC Company Standard Format.”

## **LENGTH**

**Card Length** – This represents the total number of characters that will be recognized by the system. It includes:

- **Start Sentinel** – This character must be a hexadecimal B and indicates the beginning of the card data stream. It is always considered to be at offset zero when describing the positional characteristics of the card data stream.
- **Field Separator** – This character must be a hexadecimal D and indicates that a field has ended and/or a new field is beginning. Field Separators are ignored in PassPoint format definitions and are represented by an unused character or X in the Data

Layout area. Field Separators are not necessary to separate fields.

- End Sentinel – This character must be a hexadecimal F and indicates that this is the end of the card data stream. These characters are also ignored in the PassPoint format definitions, and are treated the same way as Field Separators.
- Checksum – This character can be any single hexadecimal value (0 through F) and is found immediately after the End Sentinel. This character is not used by the PassPoint Access Control System, but must be recognized as a character placeholder in the Card Length value.

**Card Length Exact Digits** – When this box is checked, the number of characters read from the card must match the Card Length value exactly. Otherwise, the card read will be ignored. Note that many magnetic stripe cards have zeroes programmed before the Start Sentinel and after the checksum and End Sentinel. These zeroes will be ignored by the system and will not be computed as part of the exact number of digits read from the card. This is because the number of leading and trailing zeroes can vary from card swipe to card swipe. They are also used to help synchronize the card read with the interface equipment.

## **FACILITY CODE**

This field is also referred to as the Site code or System code. It is feasible for a particular company to have two or more locations. Each of the locations can have its own Facility Code to help describe the site to which they belong. It also permits the system to distinguish identical card numbers from each other.

**Start** – This value represents the offset (from zero) that the Facility Code actually begins. Recall that the Start Sentinel is always at offset zero. If this value is set to zero, it implies that the

Facility Code does not exist (or is not used) in this particular format definition.

**Length** – This value represents the number of digits that are used in the Facility Code. PassPoint will accept values from 1 to 9.

### **CARD NUMBER**

The Card Number field is generally used to distinguish one cardholder from another. It should be unique at each site, but can be duplicated if Facility Codes and/or Issue Levels are used.

**Start** – This value represents the offset (from zero) where the Card Number field actually begins. Recall that the Start Sentinel is always at offset zero. If this value is set to zero, it implies that the Card Number does not exist (or is not used) in this particular format definition. The Card Number field should *always* be used in any format definition.

**Length** – This value represents the number of digits that are used in the Card Number. PassPoint will accept values from 1 to 16. It should be noted here that the maximum number of characters that PassPoint is able to represent is 16. This value includes the Issue Level field, as well (described below). As the number of digits increases in the Issue Level field, the number of digits decreases by the same amount in the Card Number field, so that the total combined number of digits cannot exceed 16. Keep this in mind while you are defining your card format.

### **ISSUE LEVEL**

The issue level is typically used when the card number must be preserved even though the original card itself has been lost. Sometimes the Card Number is the same as an employee number

or Social Security number. If the employee loses his or her card, you can not expect them to acquire a new Social Security number to conform to the requirements of the access control system. If a card is lost, the Issue Level can be incremented, and the card number and facility codes can remain the same as they were before the loss.

**Start** – This value represents the offset (from zero) where the Issue Level actually begins. Recall that the Start Sentinel is always at offset zero. If this value is set to zero, it implies that the Issue Level does not exist (or is not used) in this particular format definition.

**Length** – This value represents the number of digits that are used in the Issue Level. PassPoint will accept values from 1 to 16. It should be noted here that the maximum number of characters that PassPoint is able to represent is 16. This value includes the Card Number field, as well (described above). As the number of digits increases in the Issue Level field, the number of digits decreases by the same amount in the Card Number field, so that the total combined number of digits cannot exceed 16. Keep this in mind while you are defining your card format.

## DATA LAYOUT

The Data Layout area provides a graphical representation of the field assignment. In addition to indicating where in the data stream each of the fields will reside, it can also alert the user to conflicts or overlaps in the format definition.

The color-coded legend at the top of the Data Layout area describes the significance of each of the fields. If any of the fields overlap due to length or offset conflicts, the overlapping areas turn red and contain an exclamation point for each overlapping

character. PassPoint *Plus* does not allow you to save a definition that has overlapping fields.

## **FACILITY CODES**

PassPoint provides the ability to define up to 16 different Facility Codes per format definition. The values placed in these fields appear in the Card Calculator. There, they can be assigned to the appropriate badge when it is commissioned.

In the event that more than 16 Facility Codes are required, the badge format can be duplicated up to three more times (for a total of four identical definitions). In this way, if the same format is used at a single account, that account can identify up to 64 unique Facility Codes.

## **LOAD FROM FILE**

Selecting this button loads a saved format definition from disk into the current format definition. Multiple formats can be made identical, as described in the Facility Codes description above. Additionally, other accounts can load these in, so that a previously defined format can be used for multiple accounts. All of the information shown on each of the Format Definition tabs will be replaced. This includes the list of Facility Codes.

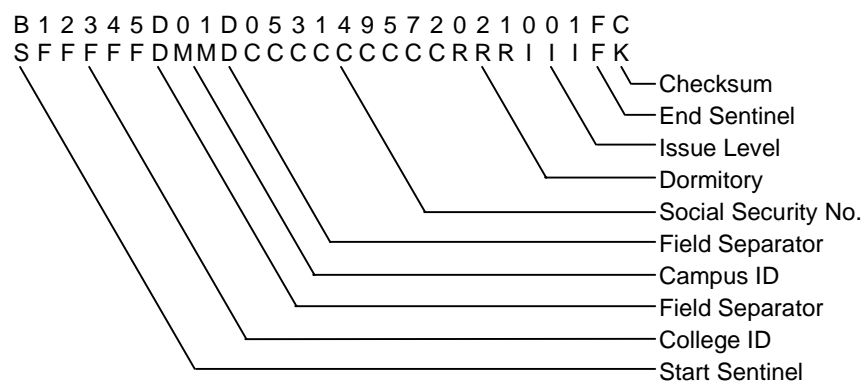
## **SAVE TO FILE**

Selecting this button saves a format definition from the currently selected format definition to disk. All of the information shown on each of the Format Definition tabs is saved. This includes the list of Facility Codes.

## ***ABA MagStripe configuration sample***

The following is a hypothetical implementation of a magnetic stripe format for a college environment.

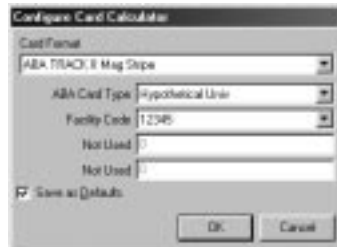
The college has five different campuses, and each campus has a number of dormitories. Each student is enrolled according to his or her Social Security number. To accommodate card loss, an issue level field has also been included. The format and typical cardholder's data is shown below.



The College ID (12345) will be used as the Facility Code. The student's Social Security number (053-14-9572) will be used as the Card Number. The Issue Level (001) will be used as the Issue Level. All other fields will be ignored. The resultant format screen would look like this:

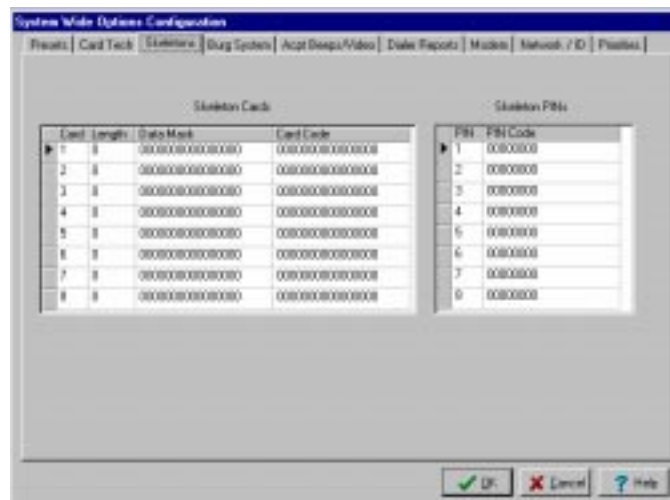


The following two screen dumps represent an example of the cardholder's record, as programmed into PassPoint.



## ***Skeleton codes (Skeletons tab)***

This screen allows the installer to edit the system's skeleton cards and skeleton PINs:



Skeleton codes are a method by which the system can grant access to specific PIN codes or cards and/or specific groups of cards in the rare event that the system experiences a communications failure between a DCM and the MLB. Skeleton cards are subjected to a bit-wise analysis as defined by the installer. This

analysis compares the fields within the encoded card data stream (the actual data read from the card) against a card data mask, and then against a specific bit pattern (card code).

After a card is read, the data from the card is compared with each of the eight entries in the skeleton card table described below. The comparison is performed in the order that the table entries appear. There are four programmable fields used during the comparison. They are Length, Data Mask, Card Code, and PIN Code. The first three fields are used to evaluate the card data stream. The last field is used to evaluate a series of digits entered through a keypad.

First, the overall length of the card is defined to the system. Up to eight different card lengths can be defined. Card data streams not matching the lengths defined are ignored. If a mismatch occurs, the process then continues on to the next entry in the table until either a match occurs or the last entry in the table has failed.

A Card Data Mask is provided to filter out the specific fields of interest. Where a one appears in a bit position of the filter, a bit in the same position of the card data stream (of matching length) is compared with a bit in the matching position of the Card Code. Where a zero appears in a bit position, that bit is ignored during the comparison process.

Card Codes (whose bit position in the Skeleton Cards Data Mask are set to a one) must match the filtered card data stream exactly, bit-for-bit. In this way, if the Data Mask consists of all ones in the area of the facility code (also referred to as the site code), any card with a matching facility code is accepted.

Once a match has been found, the row of the Skeleton Cards table that contains the matching Data Mask and Card Code fields is used to indicate the same row of the Skeleton RCM, Reader A RCM Operation by Skeleton (or Reader B RCM Operation by Skeleton),

Cards column. Once that row is identified, the operation defined in that row is executed. In other words, if a card presented to Reader B were found to match the skeleton card data in the second row of the table, and the second row of the Reader B RCM Operation by Skeleton, Cards column contained the Unlatch command, the access point that uses Reader B would unlatch (go into Bypassed mode).

Some of the terminology used in the RCM Skeleton mode differs slightly from terms used in normal operation. A Grant still grants access. An Unlatch places the door in the Bypassed (or free access) mode. A Latch places the door in the Protect mode after the access point executes a Grant sequence. The “Latch Protect after Grant” sequence allows the cardholder to exit through an unlatched door before setting the access point to the protected state.

If a reader is a combo card/pin reader, the card must match according to the criteria defined above, and any PIN number must be typed in. PINs are not checked for accuracy, just for the correct number of digits.

There are also PIN fields on the skeleton screens. The PIN fields are used only if a combo reader is in PIN-only mode, and the reader attached to that access point is (or has) a keypad. The PIN code entered into the PIN Code field of the system menu operates the same way as the normal PIN fields. That is, a four-digit PIN is left-justified. A PIN of 1234 would appear as 12340000 in the PIN Code column (assuming the system used four digits for the PIN code).

A matching PIN-only entry causes performance of the operation that appears in the same relative position of the Reader A RCM Operation by Skeleton (or Reader B RCM Operation by Skeleton) table. For example, if a PIN entered through Reader A matches the

PIN in the third row of the System, Skeleton PINS, PIN Code column, the action programmed in to the Door Control Module (DCM) Setup screen, Skeleton RCM tab, Reader A RCM Operation by Skeleton, PINs column, third row, will be executed on the appropriate access point.

The options are the same for cards as they are for PINs. They can be Not Used, Grant, Latch, or Unlatch.

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

### ***Creating and assigning skeleton card codes***

Skeleton card codes work somewhat differently from skeleton PIN codes. There are eight skeleton card codes, but because 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 Card Code is the bit pattern that is compared to 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.



---

A 1 in a bit position of the data mask means that bit position of the card code and card read must be identical.

---

When a card is read by the access point in RCM, it is then passed through the Card Data Mask filter. The resulting value (Filtered Card Data Stream) is checked against the Card Code. An EXACT

match between the Filtered Card Data Stream and 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 an access point called Front Door. Additionally, in the following examples, assume that the card number is 1827 (decimal).

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.

	P	F								C																		P
BIT POSITION	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	1

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS F = FACILITY CODE C = CARD NUMBER

Because you want to look at the Facility Code of all cards that are detected by the access point's reader, 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 Card Data Mask like this:

**NOTE:** Only the lower 26 bits are used in the Card Data Mask and Card Code.

	P	F								C																P
BIT POSITION	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
FILTER POSITIONS FOR FACILITY CODE TO PASS THROUGH		1	1	1	1	1	1	1	1																	
UNUSED POSITIONS TO BE BLOCKED BY FILTER	0									0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ACTUAL CARD DATA MASK	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CARD DATA MASK HEX EQUIVALENT	1	F								E								0								0

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS F = FACILITY CODE C = CARD NUMBER

And set up your Card Code like this for a facility code of 41 (decimal) or 29 (hexadecimal):

	P	F								C																P
BIT POSITION	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CARD CODE	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CARD CODE HEX EQUIVALENT	0	5								2								0								0

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS F = FACILITY CODE C = CARD NUMBER

The Card Code (52000 Hexadecimal) provides a match on the filtered card data stream as shown below:

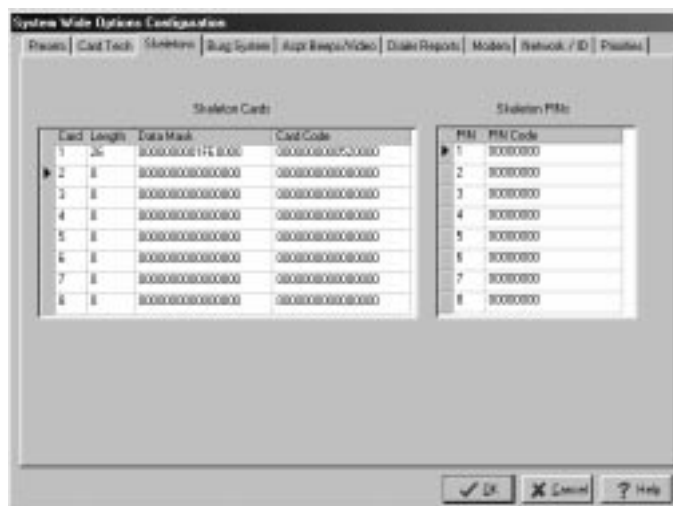
	P	F										C										P				
BIT POSITION	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CARD DATA STREAM	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	1	0
CARD DATA MASK	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FILTERED CARD DATA STREAM	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CARD CODE	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FILTERED CARD DATA STREAM AND CARD CODE HEX EQUIVALENT	0	5					2					0					0					0				

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS F = FACILITY CODE C = CARD NUMBER

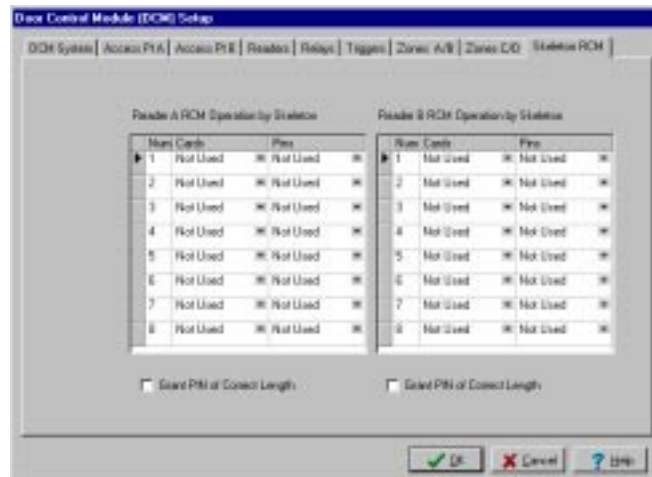
Length	Card Data Mask	Resulting Card Code
026	0000000001FE0000	0000000000520000

Now that the Data Mask (1FE0000 Hexadecimal) and Card Code (520000 Hexadecimal) have been determined, the data must be input into the system in the Skeletons screen. In the Card 1 line of the screen, enter a Length of 26, Data Mask of 1FE0000, and Card Code of 520000. The screen appears as shown below:





The next step is to make the Skeleton Card recognizable by the access point (called Front Door in this example) so that, if the system ever goes into RCM mode, cardholders with the proper facility code can obtain entry through the Front Door (called Reader A). The access point is configured using the Door Control Module (DCM) Setup, Skeleton RCM Tab screen that is shown below. For an explanation on how to reach the Door Control Module (DCM) Setup screens and a complete description of them, refer to the chapter titled “Adding a Door Expansion Kit” in this manual.



In this screen for NUM 1, we click the down arrow under Cards and select Grant and then select *OK*. Now, when the card is read, it will be filtered to obtain the facility code and then the resulting filtered data will be compared to the Card Code. An EXACT match between the Filtered Card Data Stream and Card Code will be accepted by the access point if the system goes into RCM mode. Note that we assigned the NUM 1 because this is the Skeleton Card Number that we created. If we were using multiple skeleton cards, the number we select on this screen must match the desired skeleton card number that we want to perform this function.

In other words, if we defined a particular pattern in the fourth row of the System Wide Options, Skeletons screen, the action defined in the DCM Setup, Skeleton RCM, Reader A RCM, Cards field in row four would be performed when a matching card was presented to Reader A of that DCM. There is a one-to-one mapping between the rows of these two tables.

In the next examples (A and B), let's assume that we are using the standard ADEMCO format of 34 bits. The standard ADEMCO format consists of three fields, as described below:

**Facility Code:** An eight-bit binary value that is generally the same for all cards at a particular facility. Using this field in this way, there can be a card number one at company A, as well as a card number one at company B, yet neither card will work at the other's facility.

**RCM Code:** A four-bit field that can be used to group cards with identical patterns in this field. These different groups can then be permitted to perform specific functions. This field has not yet been implemented within the framework of the system.

**Card Number:** A twenty-bit value used to indicate the card number of the card being presented.

There are also parity bits (one at the beginning and one at the end of the card data stream). These are used to authenticate the validity of the card data stream when it is transmitted from the reader to the controller. For RCM Skeleton operations, the parity bits can be ignored, depending upon the card set in use.

Example A represents a card data stream from an ADEMCO card that has a Facility Code of 8, an RCM code of 4, and a Card Number of 1827 (Decimal [723 Hexadecimal]). The total length of the Card Data Stream is 34 bits. If we wanted to use just the Facility Code to grant access in RCM, we would need to generate a

mask that has the bits that represent the Facility Code set to a 1, and all others set to a 0. The Data Mask would look like Example B.

### Example A

FIELD NAME	P	F								R				C																P				
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

### Example B

FIELD NAME	P	F								R				C																P				
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0
DATA MASK	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

*The Data Mask must now be converted to a hexadecimal number:*

DATA MASK 0 1 1 1 1 1 1 1 1 0

FIELD NAME	P		F								R				C																F					
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1		
DATA MASK	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
HEX EQUIVALENT	1		F								E				0				0				0				0				0				0	

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER



as well as the Card Code:

FIELD NAME	P	F								R	C																P							
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0
CARD CODE FOR A FACILITY CODE OF 8	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HEX EQUIVALENT	0	1				0				0				0				0				0				0								

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

Now, by placing a value of 34 in the Length field, a value 1FE000000 (Hexadecimal) in the Data Mask field, and a value of 10000000 (Hexadecimal) in the Card Code field, any ADEMCO card with a Facility Code of 8 will perform the operation defined in the relative Skeleton RCM row for that reader.

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

When you want a skeleton card to be an exact match, you must set all bits to ones (except the parity bits) in the card data mask; and you must enter a hexadecimal value of the card data stream as it is read from the card into the card code field. The following example represents a 34-bit card whose number is, in hexadecimal, 010800E46.

Original Card Data Stream:

FIELD NAME	P	F								R			C																F						
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	1	1	0

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

*Card Data Mask:*

FIELD NAME	P	F								R				C																P					
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	1	1	0
DATA MASK	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

*The Data Mask must now be converted to a hexadecimal number:*

DATA MASK 0 1 1 1 1 1 1 1 1 0

FIELD NAME	P	F						R		C																P								
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
DATA MASK	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	
HEX EQUIVALENT	1	F						F		F		F		F		F		F		F		F		F		F		F		E				

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

*as well as the Card Code:*

FIELD NAME	P	F								R			C																P						
BIT POSITION	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
CARD DATA STREAM	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	1	1	0
CARD CODE FOR AN EXACT MATCH	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	0	0	0	1	1	0
HEX EQUIVALENT	0	1				0				8				0				0				E				4				6					

NOTE: FIELD NAMES ARE AS FOLLOWS:

P = PARITY BITS

F = FACILITY CODE

R = RCM CODE

C = CARD NUMBER

Now, by placing a value of 34 in the Length field, a value 1FFFFFFE (Hexadecimal) in the Data Mask field, and a value of

10800E46 (Hexadecimal) in the Card Code field, card 1827 (decimal) with a Facility Code of 8 and an RCM Code of 4 will perform the operation defined in the relative Skeleton RCM row for that reader.

The use of skeleton card codes to obtain an access grant, access point latch, or access point unlatch is described briefly in this chapter in the previous example for 26 bit codes. It is also detailed under the Skeleton RCM tab in the “Adding a Door Expansion Kit” chapter of this manual.

### ***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.

Using skeleton PIN codes to obtain an access grant, access point latch, or access point unlatch is described under the Skeleton RCM tab in the “Adding a Door Expansion Kit” chapter of this manual.

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

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



### ***Burg configuration***

**Alarm Sounder Relay** – Click the down arrow at the right of the Alarm Sounder Relay field and from the list presented, select 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 activates in response to a burglary condition. The alarm bell can be silenced by issuing a *Disarm* command while the bell sounds. The alarm bell turns off automatically after this time expires.

**Burglary Trigger** - Click the down arrow at the right of the Burglary Trigger field and from the list presented, select 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 is on when there are no pending alarms. Electrically, the trigger draws current; that is, it measures as a logical low if it is measured with a Voltmeter when a pull-up resistor is used.

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

**Open/Close Trigger** - Click the down arrow at the right of the Open/Close Trigger field and from the list presented, select 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 is on when the system is Armed Away or Stay. Electrically, the trigger draws current; that is, it measures as a logical low if it is measured with a Voltmeter when a pull-up resistor is used.

The Open/Close Trigger is off when the system is disarmed. Electrically, the trigger does not draw current; that is, it measures 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** - Because all actions on a connected VISTA alarm panel are logged to the VISTA's event history log, any action that the PassPoint system initiates on the VISTA panel must be mapped 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 you want the system keypad to sound slow beeps in the event ANY module in the PassPoint system loses AC power.

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

**Com Failure** - Check this box if you want the system keypad to sound slow beeps in the event 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 is listed. Set the selection boxes in the appropriate column in order to indicate the access points that you want to sound Door Open alarms and Door Open timeouts. If your

computer 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 make selections in the *Camera* column only when you have the appropriate video capture equipment installed.

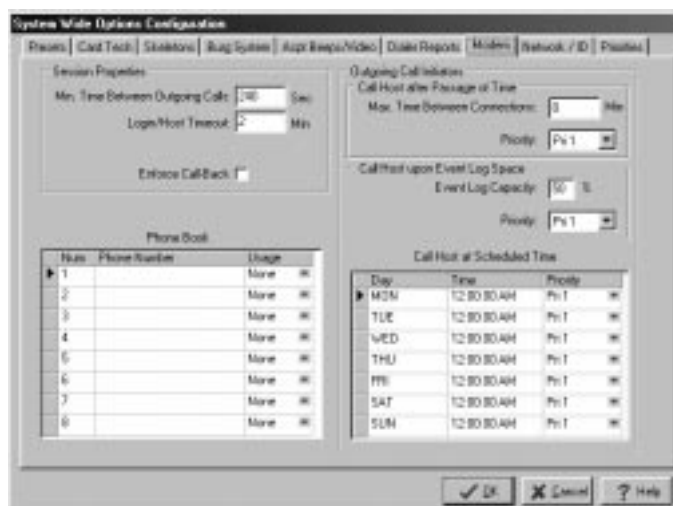
---

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

This screen sets 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 are communicated to the central station by the VGM or a connected VISTA panel. This screen pertains only to systems that are using a VGM.

## ***Modem options (Modem tab)***

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



## ***Session properties***

**Min Time Between Outgoing Calls** - This is the minimum number of seconds allowed between outgoing calls made by the PassPoint system. This setting establishes a window of time when someone may call in to the PassPoint system, even when the system is busy making outgoing calls. This time pertains only to the interval between successful outgoing calls. 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, forces a re-negotiation of a connection with a Computer Host System (in a future version of the product). When a remote connection is used, if this timeout time passes without someone logging in, the system terminates 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 you are using a modem connection. Do not set this field to a non-0 value if you are using a hardwired 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 because any dial-in that is answered by the PassPoint terminates and the system initiates 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 computer. You need not fill in these numbers if the only computer 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 calls after a call-in is received.

All other numbers are used to dial a particular computer when an event of a particular priority threshold occurs. This allows the system to call different hosts to handle different types of events.

### ***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 initiates 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 generates an outgoing call of the indicated priority.

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

The PassPoint system initiates 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:

The screenshot shows a software window titled "System Wide Options Configuration" with a tabbed interface. The "Network/ID" tab is selected. The window contains two main sections: "Network" and "Identification".

**Network Section:**

- Subnet Number:** A text input field containing the value "1".
- Header Snipe Timeout:** A spin box set to "3" with a unit dropdown menu showing "Sec".
- Host Identification:** A text input field containing "FFFFFFFF" with a small "..." icon to its right.
- Warning:** A line of text below the Host Identification field reads: "... Do not change this field without making the appropriate change in the system information."

**Identification Section:**

- Expanded Caption:** A text input field containing "PassPoint ACS".
- Primary Subscriber Acct #:** A text input field containing "000101".
- Sec Subscriber Acct #:** A text input field containing "000000".

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

## **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 waits after a card is swiped or a PIN is entered. Under normal circumstances, the MLB responds 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 resets. The default setting is 3 seconds. You should set this default setting higher if you are doing visual verification.

**Host ID** - This 12-hexadecimal-digit number is used to validate a connection with the PassPoint *Plus* software. The number set here **MUST** match the number set for the computer software in order for uploads/downloads and event capturing to operate.

Although the Host ID has an initial value of “FFFFFFFFFFFF,” the installer should change it 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 are 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.

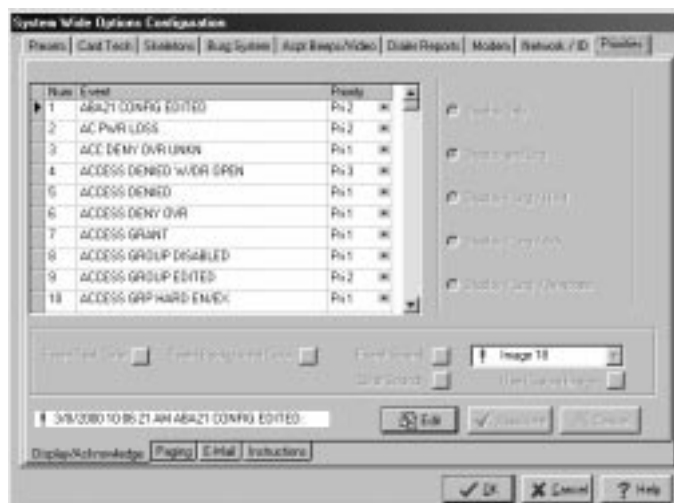
**Secondary Subscriber Account Number** - Enter in the secondary account number for this account. The first four digits of this number are sent to your secondary central station monitoring service in the event that a call to the central station is warranted, and the primary central station is not responding. 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 are not 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 transmits 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 could affect remote connections. Altering the event priorities can cause outgoing calls to the host, and can prevent events from being logged. Additionally, many events that have a fault/restoral characteristic only show up once in the list. Changing the priority for one changes the priority for both (i.e., Access Point Door Open and Alarm Restore).





The priorities screen may be used to change an event's priority, change an event's attributes, define event paging, define event e-mail, and create event instructions. Procedures for performing these actions are provided in the following paragraphs.

### ***Changing an Event's Priority***

To change an event's priority:

- 1. Scroll through the event listing provided in the event grid until you reach the event where you want a priority change.**
- 2. Click on the down-arrow at the right side of the event listing.** A priority listing is displayed.
- 3. Click on the priority level desired.** The priority for the event is changed.

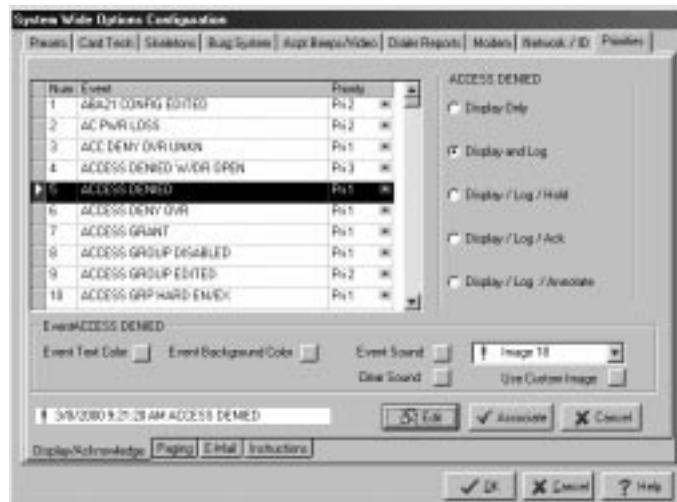


It is important to note that setting an event priority to 0 will override and cancel any other event attributes, since an event with a priority of 0 will in essence, never occur and will not even be displayed.

4. Repeat steps 1 through 3 for each event to be changed.

### ***Changing an Event's Attributes***

1. Scroll through the event listing provided in the event window until you reach the event where an attribute change is desired.
2. Choose an event by clicking in the left-most column in the event grid. The whole event row will be highlighted, as shown below, when an event has been selected.
3. Click the *Edit* button. This enables the buttons on the form.



4. Edit the attributes for the event using the buttons on the screen. The buttons have the following functions:

<i>Event Text Color</i>	Click this button to change the color of the textual part of the event.
<i>Event Background Color</i>	Click this button to change the background color of an event.
<i>Event Sound</i>	Click this button to associate a wav file to be played on the event. Use short wav files.
<i>Clear Sound</i>	Click this button to disassociate a wav file from an event.
<i>Images</i>	There are 46 factory-shipped images in the list that can be associated with an event.
<i>Custom Image</i>	You can create your own bitmap image and associate it with an event. The created image must be 15 x 15 pixels.
<i>Display Only</i>	The event is to be displayed only and not saved to the database for reporting at a later date.
<i>Display and Log</i>	The event is to be displayed and saved to the database.
<i>Display/Log/Hold</i>	The event is to be displayed and saved to the database. It will also be held in the priority bucket of its corresponding numerical priority.
<i>Display/Log/Ack</i>	The event is to be displayed and saved to the database. It will be held in the priority bucket of its corresponding numerical priority. This event will also require acknowledgement.

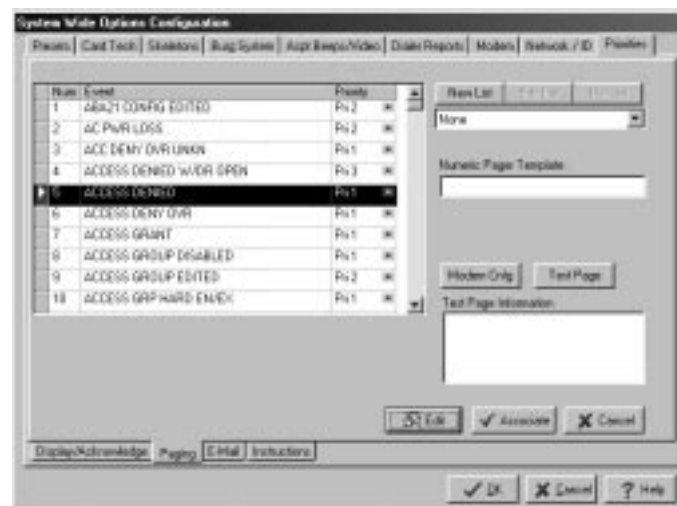
*Display/Log/  
Annotation*

The event is to be displayed and saved to the database. It will be held in the priority bucket of its numerical priority. This event will also require annotation.

5. When you have finished editing the event attributes, click the *Associate* button to associate the changes you made to an event.
6. Repeat steps 1 through 5 for each event for which you want to change the attributes.

## Defining Event Paging

In order to use the paging feature of PassPoint, the host PC must always be connected to MLB. To setup PassPoint to page on an event, you need to configure your modem and then create a paging list. When you click on the paging tab, the following screen is displayed.



### **Configuring the Modem**

1. **Attach a modem to an available communications port on your computer.**
2. **Click on the *Modem Cnfg* button.** The following screen is displayed.



3. **Set the communications port that your modem is plugged into by selecting it from the *Modem Port* drop-down list.**
4. **Set the *Dial string* to ATDT for tone dialing and ATDP for pulse dialing.**
5. **Leave the *Init String* field blank for now.** With this blank, the Modem will send an AT+ and return. If this default does not work, you will need to find the modem's manual. Most paging terminals use older modems that cannot accept error correction protocols of the newer V.xx modems. Therefore you need a modem initialization string that will set the modem to the Normal Bell 212 mode.
6. **Set the *Baud Rate* field to the paging terminal baud rate.** (2400 works well for PageNet.)

### **Creating a Paging list**

1. **Scroll through the event listing provided in the event window until you reach the event where paging is desired.**

2. Choose an event by clicking in the left-most column in the event grid.
3. Click the *Edit* button. This enables the *New List* button.
4. Click the *New List* button. This opens the *Pager List Members* dialog shown below:



5. Enter the name of the paging list in the *List Name* edit box.
6. Enter the *Pager Pin*.
7. Enter the *Pager Access #*. (Paging terminal's phone number.)
8. Click the + button. This moves your entry to the *Members* list.
9. Right-click on the pager in the *Members* list. A dialog box is presented for pager type selection (alpha or numeric). Select the type that matches your pager.
10. Repeat steps 1 through 9 for each event and/or pager desired..
11. Click the *OK* button to save the list.

This list can now be associated with many events.

**NOTE:** The existing list can be edited by using the *Edit* button.

### ***Using The Numeric Pager Template***

The text that goes to the pager is the actual event text plus the account number in an alphanumeric pager. When you have a numeric pager, you must use the *Numeric Pager Template*. The *Numeric Paging template* uses place holders:

%A to substitute the account number

%T to substitute the resource type (1=Access Point, 2= Reader, 3 = Relay, 4=Reader, 5=Trigger)

%R to substitute the resource number

For example, if the account number is 1234 and the event is an access point Door Open Alarm, you can construct your template to look like this:

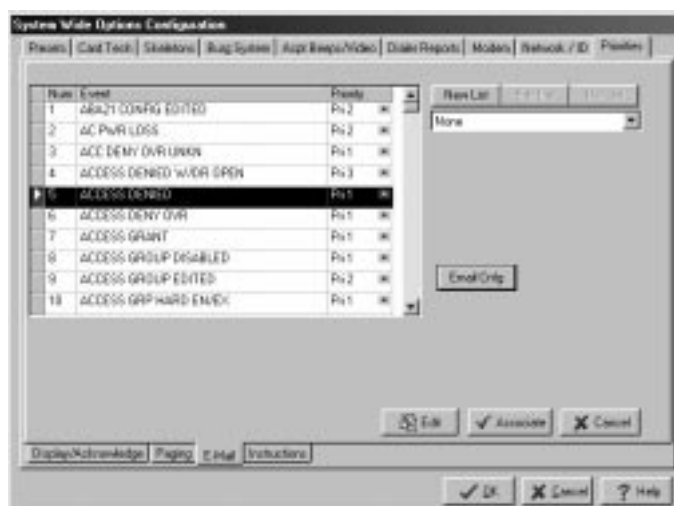
911 %T %R 000 A%

This will be paged as:

911 1 1 000 1234

### ***Defining Event E-mailing***

In order to use the e-mail feature of PassPoint, the host PC must always be connected to MLB. Additionally, you must have network access to an SMTP (Simple Mail Transport Protocol) server to setup PassPoint to e-mail on an event. To set up PassPoint to e-mail on an event, configure your e-mail and then create an e-mail list. When you click on the e-mail tab, the following screen is displayed:



## Configuring E-mail

1. Click on the *Email Cnfg* button. The following *Email Configuration* screen is displayed:



2. Enter the address of your SMTP host in the *SMTP Host Address* field.
3. Enter the user name that might be needed to gain access to the SMTP server in the *User ID* field.
4. Enter the address you want to use as the sender's address in the *From Address* field.



5. Enter the text that you want to be appended to the end of the event text on the subject line of the e-mail in the *Subject Post Text* field.
6. Click the *OK* button.

### ***Creating an E-mail List***

1. Scroll through the event listing provided in the event window until you reach the event where e-mail is desired.
2. Choose an event by clicking in the left-most column in the event grid.
3. Click the *Edit* button. This will enable the *New List* button.
4. Click the *New List* button. This will open the following *Email List* dialog:



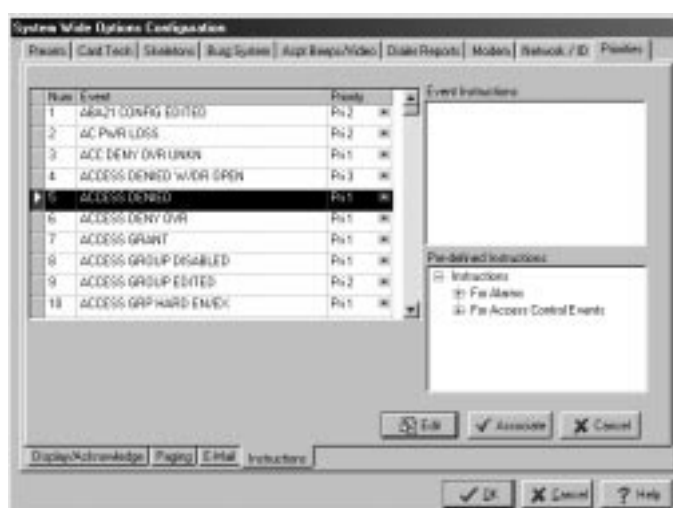
5. Enter the name of the e-mail list in the *List Name* edit box.
6. Enter the *Email Address*.
7. Click the **+** button. This will move your entry to the *Members* list.
8. Repeat steps 6 and 7 for each e-mail address.
9. Click the *OK* button.

This list can now be associated with many events.

**NOTE:** The existing list can be edited by using the *Edit* button.

## ***Creating Event Instructions***

You can create event instructions using the Instructions tab. When you click on the Instructions tab, the following screen is displayed:



You can type instructions in the *Event Instructions* edit box; you can pick an instruction from the *Pre-defined Instruction* box by double-clicking on one, or you can add your own custom instructions by right-clicking in the *Pre-defined Instructions* box and then selecting *Edit Custom Instructions*. When you select *Edit Custom Instructions*, the following screen is displayed:



After typing your new custom instructions, exit the *Edit Custom Instructions* screen, right-click again in the *Pre-defined Instructions* box, and choose *Reload Instructions*. This adds your new instructions to the listing of Pre-defined Instructions so that it may be inserted into the *Event Instruction* box.

To associate your event instructions to the selected event, click on the *Associate* button.



## Chapter

# 8

# *Resource Lists*

This chapter explains how define Resource Lists. In this chapter you will learn how to:

- **Define Resource Lists**
- **Use Resource Lists**

## Defining Resource Lists

You may create lists of the following resources: access points, readers, relays, triggers, and zones. Once configured, these resources can be controlled either independently or as a list. Each resource type may have up to 16 lists defined.

All resource lists are configured in a dedicated dialog box, called Resource List Configuration. To reach this dialog box, select *Resource Lists* from the Installer Configuration dialog box:



All of the tabs (Access Points, Readers, Relays, Triggers, and Zones) contain the following fields and buttons:

**Previous/Next** – These buttons move the system to the next or previous resource list.

**Available (Resource)** – This field displays all the available resources that may be selected to belong to a resource list.

**Name** – You may enter a name for the current resource list in this field.

**(Resource) List Configuration** – This field displays all the resources that belong to the currently selected list.

**Add >** – Clicking this button assigns the selected resource to the current list.

**All >>** – Clicking this button assigns all available resources to the selected list.

**< Remove** – Clicking this button removes the selected resource from the current list.

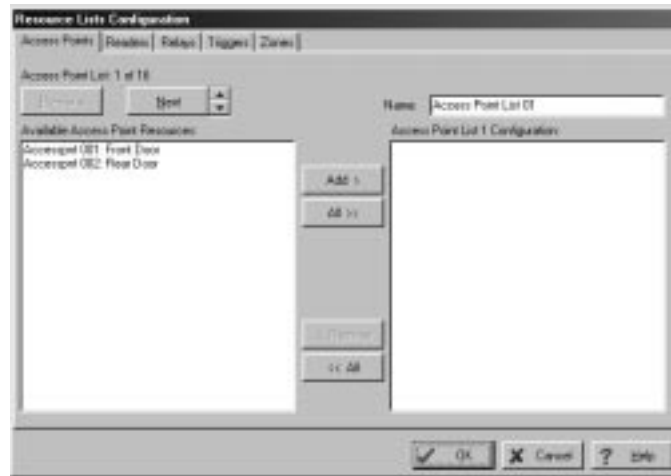
**<< All** – Clicking this button removes all resources from the selected list.

**OK** – Click this button when you are finished configuring resource lists.

**Cancel** – Click this button when you want to exit Resource List Configuration without saving any of your changes.

## ***Access Points tab***

Use this screen to define access point lists:



You can configure up to 16 access point lists. Any access point may be assigned to more than one list. To configure an access point list, proceed as follows:

1. **Select the access points listed in the Available Access Point Resources window that are to be included in the list, using method a. or b. below:**
  - a. **To select individual access points:** The access points may be selected by clicking on them. You can select multiple access points by using SHIFT-click and CONTROL-click mechanisms standard to Windows™. After access point selection, click the *ADD >* button. The selected access points appear in the Access Point List Configuration window.
  - b. **To add all access points:** Click the *ADD >>* button. The access points appear in the Access Point List Configuration window.
2. **Enter a name for the list in the Name area of the screen.**

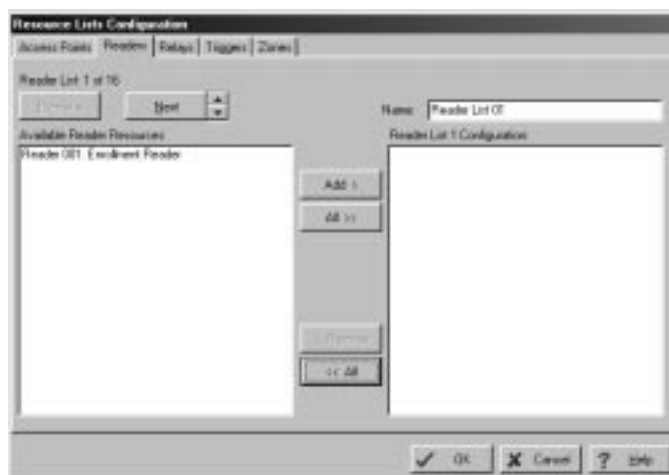


3. Click *Next* and repeat steps 1 and 2 for each access point list desired.
4. When all access point lists have been configured, you may click on one of the tabs to create lists for a different resource; or, if all lists have been configured, click *OK*. The **Installer Configuration (Hardware)** screen reappears.

When you exit the Installer Configuration screen, you are notified that the database needs to be downloaded. If you are finished configuring your hardware, follow the prompts for downloading the MLB.

## ***Readers tab***

Use this screen to define reader lists:



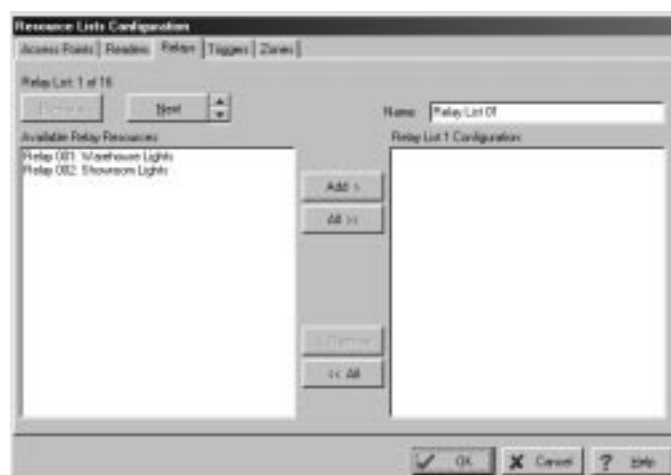
You can configure up to 16 reader lists. Any reader may be assigned to more than one list. To configure a reader list, proceed as follows:

- 1. Select the readers listed in the Available Reader Resources window that are to be included in the list, using method a. or b. below:**
  - a. To select individual readers:** The readers may be selected by clicking on them. You can select multiple readers by using SHIFT-click and CONTROL-click mechanisms standard to Windows™. After reader selection, click the *ADD >* button. The selected readers appear in the Reader List Configuration window.
  - b. To add all readers:** Click the *ADD >>* button. The readers appear in the Reader List Configuration window.
- 2. Enter a name for the list in the Name area of the screen.**
- 3. Click *Next* and repeat steps 1 and 2 for each reader list desired.**
- 4. When all reader lists have been configured, you may click on one of the tabs to create lists for a different resource; or, if all lists have been configured, click *OK*. The Installer Configuration (Hardware) screen reappears.**

When you exit the Installer Configuration screen, you are notified that the database needs to be downloaded. If you are finished configuring your hardware, follow the prompts for downloading the MLB.

## Relays tab

Use this screen to define relay lists:



You can configure up to 16 relay lists. Any relay may be assigned to more than one list. To configure a relay list, proceed as follows:

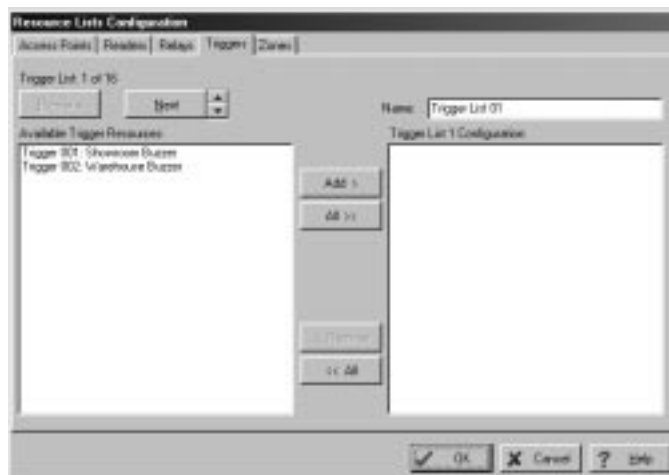
1. **Select the relays listed in the Available Relay Resources window that are to be included in the list, using method a. or b. below:**
  - a. **To select individual relays:** The relays may be selected by clicking on them. You can select multiple relays by using SHIFT-click and CONTROL-click mechanisms standard to Windows™. After relay selection, click the **ADD >** button. The selected relays appear in the Relay List Configuration window.
  - b. **To add all relays:** Click the **ADD >>** button. The relays appear in the Relay List Configuration window.
2. **Enter a name for the list in the Name area of the screen.**

3. Click *Next* and repeat steps 1 and 2 for each relay list desired.
4. When all relay lists have been configured, you may click on one of the tabs to create lists for a different resource; or, if all lists have been configured, click *OK*. The **Installer Configuration (Hardware)** screen reappears.

When you exit the Installer Configuration screen, you are notified that the database needs to be downloaded. If you are finished configuring your hardware, follow the prompts for downloading the MLB.

## ***Triggers tab***

Use this screen to define trigger lists:



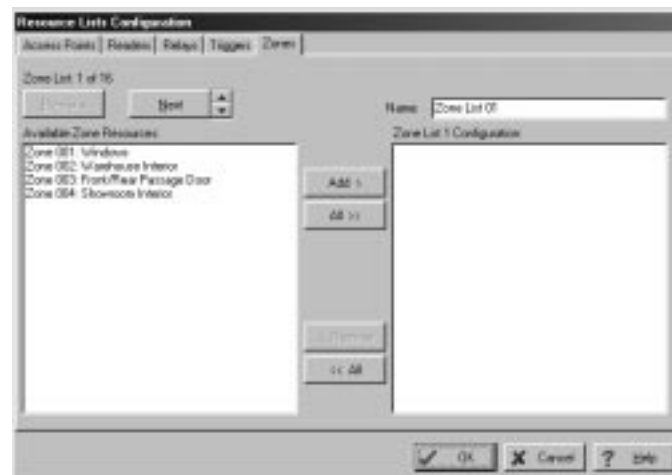
You can configure up to 16 trigger lists. Any trigger may be assigned to more than one list. To configure a trigger list, proceed as follows:

1. **Select the triggers listed in the Available Trigger Resources window that are to be included in the list, using method a. or b. below:**
  - a. **To select individual triggers:** The triggers may be selected by clicking on them. You can select multiple triggers by using SHIFT-click and CONTROL-click mechanisms standard to Windows™. After trigger selection, click the *ADD >* button. The selected triggers appear in the Trigger List Configuration window.
  - b. **To add all triggers:** Click the *ADD >>* button. The triggers appear in the Trigger List Configuration window.
2. **Enter a name for the list in the Name area of the screen.**
3. **Click *Next* and repeat steps 1 and 2 for each trigger list desired.**
4. **When all trigger lists have been configured, you may click on one of the tabs to create lists for a different resource; or, if all lists have been configured, click *OK*. The Installer Configuration (Hardware) screen reappears.**

When you exit the Installer Configuration screen, you are notified that the database needs to be downloaded. If you are finished configuring your hardware, follow the prompts for downloading the MLB.

## **Zones tab**

Use this screen to define zone lists:



You can configure up to 16 zone lists. Any zone may be assigned to more than one list. To configure a zone list, proceed as follows:

1. **Select the zones listed in the Available Zone Resources window that are to be included in the list, using method a. or b. below:**
  - a. **To select individual zones:** The zones may be selected by clicking on them. You can select multiple zones by using SHIFT-click and CONTROL-click mechanisms standard to Windows™. After zone selection, click the **ADD >** button. The selected zones appear in the **Zone List Configuration** window.
  - b. **To add all zones:** Click the **ADD >>** button. The zones appear in the **Zone List Configuration** window.
2. **Enter a name for the list in the Name area of the screen.**

3. Click *Next* and repeat steps 1 and 2 for each zone list desired.
4. When all zone lists have been configured, you may click on one of the tabs to create lists for a different resource; or, if all lists have been configured, click *OK*. The **Installer Configuration (Hardware)** screen reappears.

When you exit the Installer Configuration screen, you are notified that the database needs to be downloaded. If you are finished configuring your hardware, follow the prompts for downloading the MLB.

## ***Using Resource Lists***

Once a Resource List has been configured, it appears under the Resource Lists heading in the system tree on the main PassPoint screen. Clicking on a list provides you with many of the same options that you would see if you selected an individual resource. The difference is that you will perform an operation on all resources in the list. For example, if you click on an access point list and select *Bypass*, all access points in the list will be bypassed.





## *Section Two*



## *Expanding PassPoint*



## Chapter

# 9

## *Adding a Door Expansion Kit*

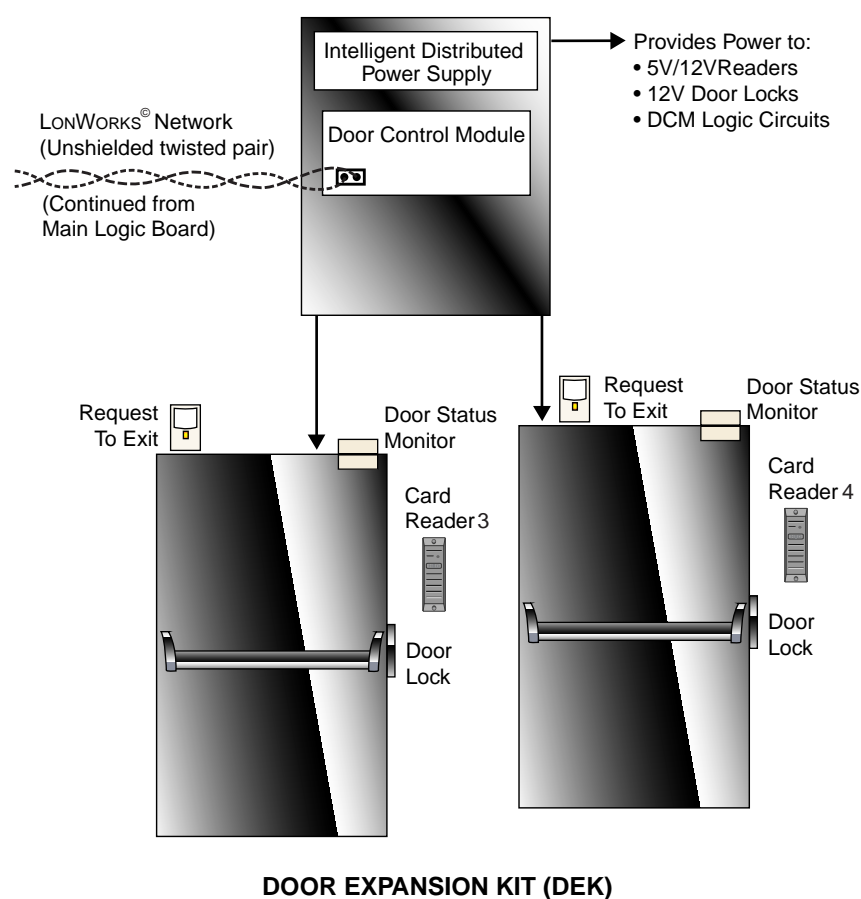
Adding a Door Expansion Kit (DEK) allows you to quickly add two more access points to an existing PassPoint installation.

In this chapter you will learn how to:

- **Mount the DEK control panel**
- **Wire all of the components of the DEK**
- **Activate and set up the DEK**
- **Enroll the DEK into an existing PassPoint system**

## Understanding Your Door Expansion Kit

The PassPoint Door Expansion Kit allows you to quickly add two more doors to your existing PassPoint installation. Essentially, the DEK consists of a Door Control Module and power supply, mounted in a standard cabinet. Once the DEK is connected to your existing system, you need only to enroll the new Door Control Module and set up your new access points.



***What's in your  
Door Expansion  
Kit?***

Your PassPoint DEK consists of the following hardware components:

- **1 pre-configured access panel, consisting of the following:**
  - 1 metal enclosure
  - 1 Door Control Module
  - 1 power supply
- **1 plug-in transformer**

## ***Installing the DEK***

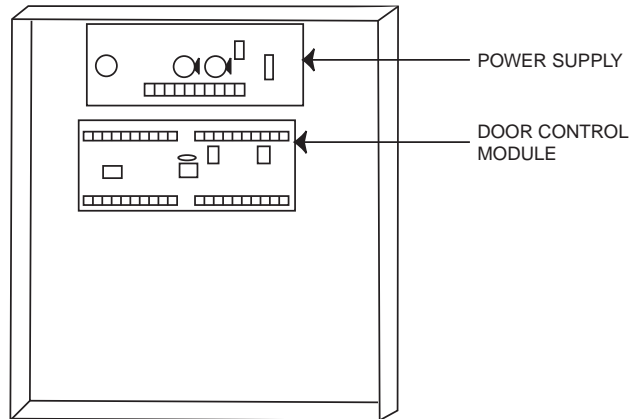
There are six simple steps to install and enroll the DEK into an existing PassPoint system. Follow each of the steps below and follow the wiring diagram provided.

### ***Step 1 - Mount the DEK panel***

The DEK panel (or cabinet) contains the kit's Door Control Module and power supply.

When the door to the panel is removed, the inside of the cabinet looks like this:

*DEK Panel with  
DCM and power  
supply.*



### ***Choosing a mounting area***

When selecting a mounting area for the panel, choose a clean, dry place not readily accessible to the general public but convenient enough so that a technician can get to the panel easily. The panel should be mounted on a sturdy wall using fasteners or anchors (not supplied in your kit).

- 1. Position the cabinet on the wall and use the holes in the back of the cabinet to mark your four mounting holes.**
- 2. Using four anchors or fasteners, mount the cabinet to the wall.**



When mounting the cabinet, be very careful not to jar the system's PC boards.

## Step 2 - Connect the DCM

Connecting the DCM involves the following steps:

- **Connecting the DCM to the power supply and system's MLB**
  - **Connecting the power transformer**
  - **Connecting card readers**
  - **Connecting DSM and RTE devices**
  - **Connecting optional 7-ampere-hour battery**
- 



When making these connections, refer to Appendix A, Wiring Considerations, for additional diagrams and system ratings.

---

### **Connecting the DCM to the MLB and power supply**

1. **Connect the *local* power jumper between power supply connector J5 and DCM connector J1.**
2. **Connect two network connection leads between the MLB and DCM.**

Connect one lead between terminal 1 of the DCM and terminal 16 of the MLB.

Connect the other lead between terminal 2 of the DCM and terminal 15 of the MLB.

---



Use twisted-pair wiring for these connections. Also, use proper termination for the modules. Refer to Appendix A for details.

---

***Connecting the power transformer***

The DEK comes with a wall-pack power transformer must be wired to the DCM. To do so:

- 1. Connect the leads of the power transformer to terminals 1 and 2 of the DEK power supply.**

***Connecting card readers***

Card readers are not included with the DEK and must be purchased separately.

Refer to the documentation accompanying your card readers for proper installation instructions. If you have purchased PassPoint proximity readers, refer to the applicable section of this guide.

***Connecting DSM and RTE devices***

Zones A through D of the DSM (terminals 5 through 10) can be used for optional Door Status Monitoring (DSM) or Request-to-Exit (RTE) devices.

***Connecting the optional 7-ampere-hour battery***

If you have purchased the optional 12-volt, 7-ampere-hour battery, install the battery and connect it to the DEK power supply.

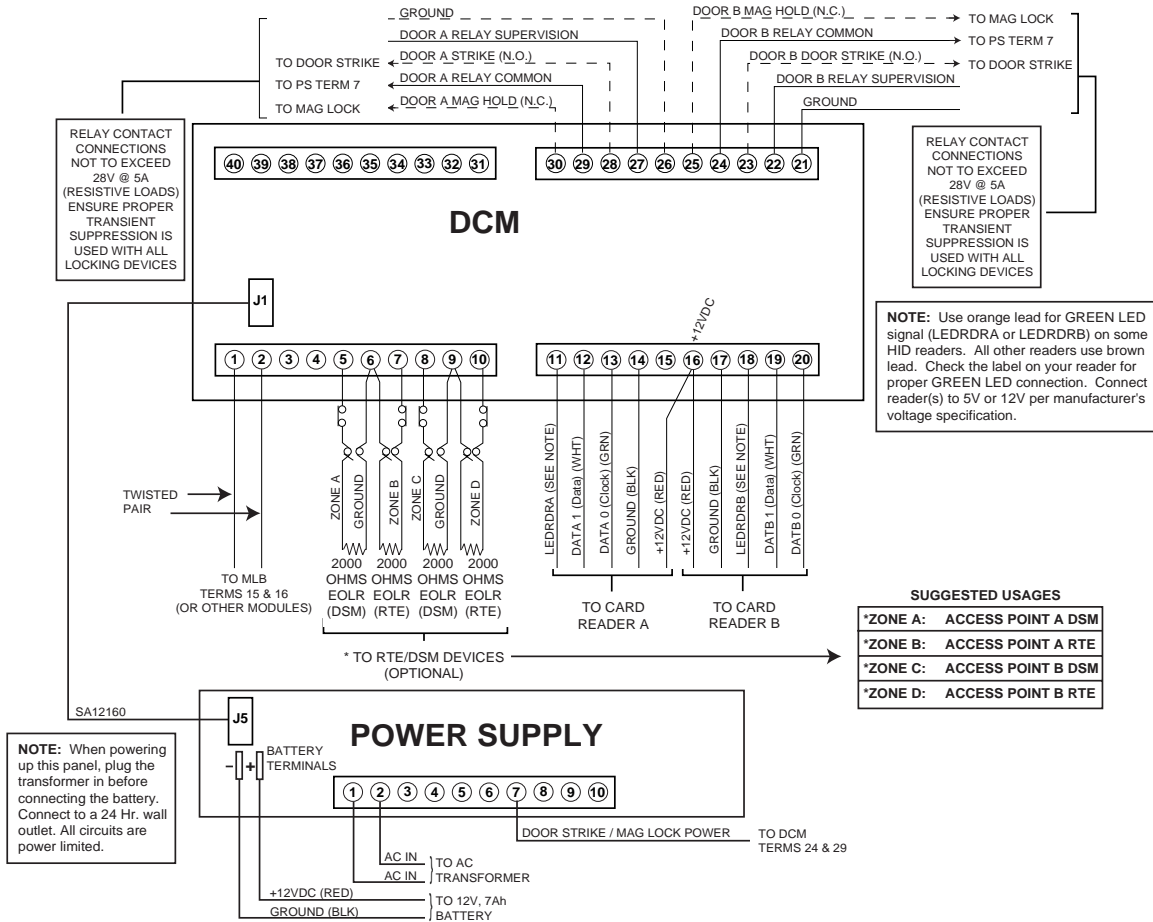


After battery installation, do not disconnect the system's wall pack for any extended period of time. To do so will discharge the battery.

---

Connect these devices according to the DCM summary of connections diagram below. Also, refer to Appendix A of this guide for applicable wiring information, and Chapter 12 for a description of the different possible zone configurations.





### Step 3 - Activate the system

Once the DCM has been connected and all door control hardware has been mounted and wired to the system, you can activate the system. To do so, plug the power transformer into a suitable wall outlet. The wall outlet must be a 24-hour (nonswitched) power source.

## Step 4 - Add and set up the DCM

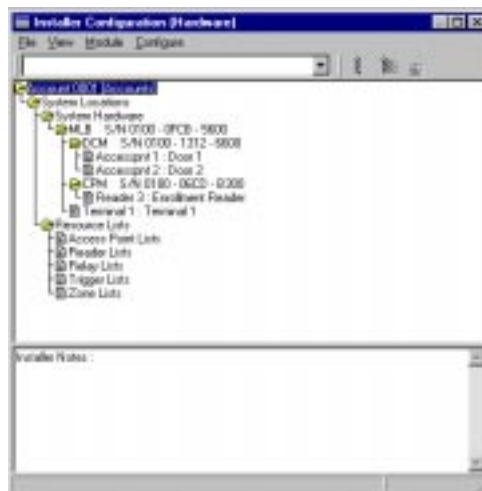
Now that the DEK is powered up, add the new DCM to your existing installation, and set up your doors. To do this, you will use the DCM Wizard.

To add and set up the new DCM, follow the procedure below:

### 1. From the *Config* menu, select *Hardware*.

The Installer Configuration dialog box appears:

Use the Installer Configuration dialog box to view/modify system components and to set various system options.

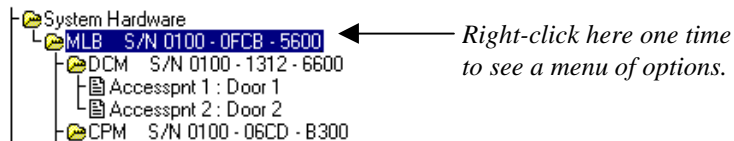


The Installer Configuration dialog box lists all of the components of the system. Here is where you add system modules such as DCMs. This dialog box is also used to set various system options, such as skeleton codes and modem settings.



Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

2. **Right-click on the MLB once or from the *Module* menu, select *Add*.**



This will bring up a menu of options.

3. **From the menu, select *Add DCM*.**

The DCM Wizard appears:



4. **Click *Next* to continue.**

Clicking *Next* always brings you to the next screen of the Wizard:



**5. Specify how many access points you want to configure.**

The Wizard gives you three options:

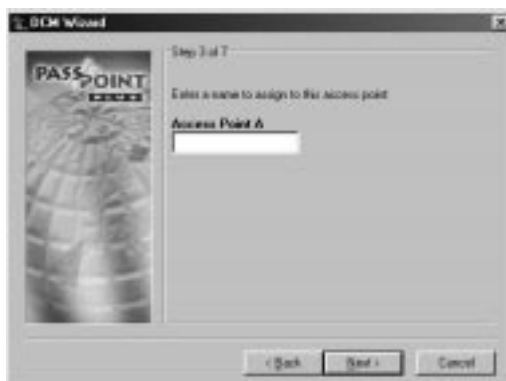
- **One Entrance Point**
- **Two Entrance Points**
- **One Entrance/Exit Point**

The option you select depends upon the needs of your installation. For the sake of this procedure, assume that you are only configuring one entry point. The procedure for configuring two access points is essentially the same.

When you have made your selection, click *Next* to continue.

**6. Enter the name of the access point.**

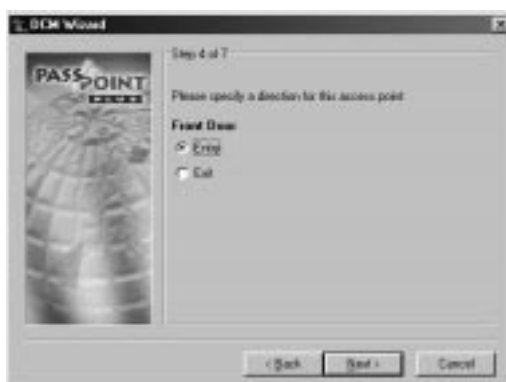
The name should be something descriptive of the door; e.g., “Front Door” or “Warehouse Door.”



Once you have entered a name for the access point(s), click *Next* to continue.

**7. Choose a direction for the access point.**

You can choose to make the access point either an entry point or an exit point:



After choosing a direction, click *Next*.

**8. Choose whether or not you want Door Status Monitoring (DSM) for the access point.**

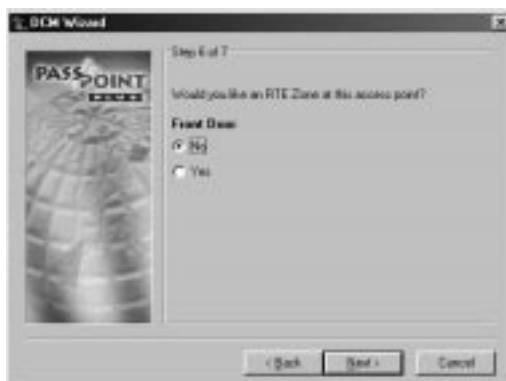


DSM is a function that allows the system to monitor how long a door is kept open, and sounds an alarm if that amount of time is violated.

If you select to use DSM for a door (as shown in this example), the system then asks you if you want to set a pre-alarm trigger for the door. The pre-alarm trigger is a warning signal that sounds before the door goes into alarm. It is used to warn individuals that the door will go into alarm if they do not close it immediately.

When you have made your DSM selections, click *Next* to continue.

- 9. Choose whether or not you want Request-to-Exit (RTE) for the access point(s).**



An RTE zone is a device connected to the door that requires system verification before allowing a cardholder to exit through the door. An RTE device may be a button for the cardholder to push, or it may be a motion detector that detects when a person is coming toward the door to exit. When the device is pushed (in the case of the button) or senses a person (in the case of the motion detector), the system unlocks the door and allows the person to exit.

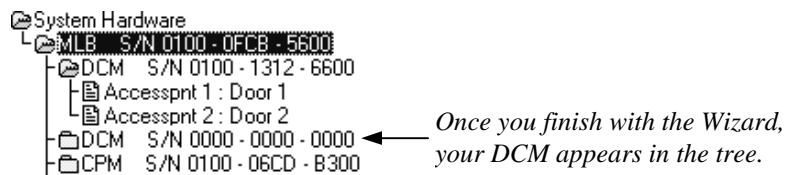
When you have made your RTE selection, click *Next* to continue. The Wizard presents a summary screen of your access point configuration choices:



**10. Click *Finish* to exit the Wizard and save your changes.**

The tree in the Installer Configuration dialog box now displays your new DCM:

**NOTE:** If this is the first DCM in your tree, the access points you defined, while using your DCM Wizard, are also shown.



Although you have configured your DCM and access points, you must still enroll the DCM so that the system recognizes it and all its configuration settings. Enrolling the DCM is covered in the next step.

## ***Step 5 - Auto enroll the DCM***

Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

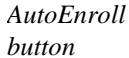
When you enroll a system module, the system goes out and searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because these modules have serial numbers that contain only zeros. For instance, look at the DCM you have just added with the Wizard. It has a serial number that contains only zeros. That means it has not been enrolled, and is not truly part of the system yet.

To enroll the DCM you just configured, follow the procedure below:



**dialog box.**

button:



shown below:



moments.

below below.

## 2a. Enrolling a Single Module.

---

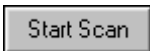
To enroll a single module into your PassPoint system, proceed as follows:

---



Never power down the MLB while the system is enrolling a module.

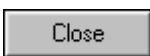
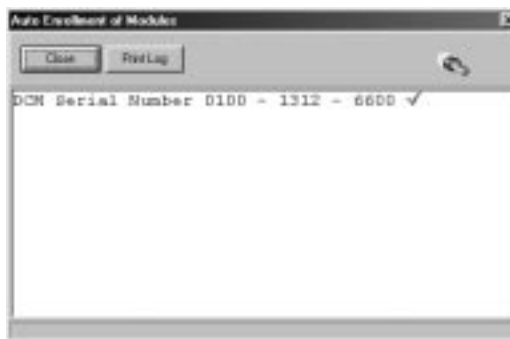
---



**(1) Click the *Start Scan* button.**

The system searches for the module. When the module is found, the system blinks the yellow service LED on the module, presents a screen message indicating that the module has been enrolled, and stops scanning for modules.

After the system has enrolled the module, a screen is presented that shows the module (with serial number) that has been enrolled.



**(2) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

## 2b. Enrolling Multiple Modules.

The Auto Enroll dialog box should already be on your screen, and should look something like this when enrolling multiple modules:



---

If the modules are powered up before the enrollment process or powered up in the wrong order, they will be enrolled incorrectly. Never power down the MLB during the enrollment process.

---


To enroll multiple modules into your PassPoint system, the modules must be powered up in the order that they are listed on the screen. To enroll the modules, proceed as follows:

A rectangular button with a grey gradient and the text "Print Log" in a sans-serif font.

(1) **Click the *Print Log* button.** A “walk list” of all the modules waiting to be enrolled is printed.

(2) **Verify the power is applied to the first module listed only.**

**NOTE:** You must power up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered up.

A rectangular button with a grey gradient and a black border, containing the text "Start Scan" in a black sans-serif font.

**(3) Click the *Start Scan* button.**

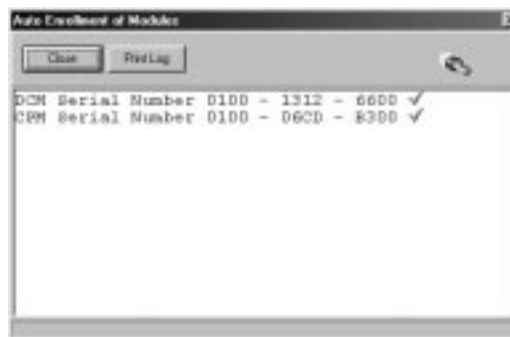
The system searches for the first module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. Next, a message will be displayed indicating that the system is polling for the next module in the “walk list.”

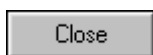
**(4) Apply power to the next module in the list.**

The system searches for the next module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. If additional modules are in the list, a message will be displayed indicating that the system is polling for the next module.”

**(5) Repeat the application of power to the modules, one at a time, until all modules have been enrolled.**

When the system has enrolled the last module in the list, the screen shows a listing of modules (with serial numbers) that have been enrolled.





**(6) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

## ***Step 6 - Download the database***

The last step to getting your DEK operational is to download the database.

Remember, the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your computer, these changes are not automatically made to the database on the MLB. They are kept in a temporary storage area on your computer until you download them to your MLB database. Any changes made on the computer must be downloaded to the database in order for them to take effect.

**1. Close the Installer Configuration dialog box.**

The system asks if you want to download the database:



**2. Click *Yes*.**

The Download dialog box appears:



At the top of the dialog box is the account number you will be downloading. There are also checkboxes in the dialog box that tell you what information you will be downloading. The system check-marks these boxes according to the system options you have changed. If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

### 3. Click *Start*.

The database download proceeds. The status bar at the bottom of the dialog box tracks the progress of the download.

## ***Configuring the DCM***

PassPoint provides a list of function for you to choose from, if you at any time you want to change the default settings of the DCM provided by the template (or Wizard), you want to expand on these settings, or you want to edit data previously

entered. Using these functions, you can configure your system DCMs in various ways.

DCMs are configured using the DCM Setup dialog box. To reach this dialog box:

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

The Installation Configuration dialog box appears.

2. **Right-click on the DCM once.**

This will bring up a menu of options.

3. **From the menu, select *Properties*.**

The DCM Setup dialog box appears:



### ***Using the DCM Setup dialog***

As you can see, the DCM Setup dialog contains nine tabs. Each tab contains fields that describe/control various functions and settings of the DCM. The tabs and their related fields are described below.

### ***DCM System tab***

**Serial Number** - You can enter the serial number for this module if you know it or leave this field set to 0000-0000-0000 to auto enroll the serial number. The serial number must be unique. Note that if you are replacing an existing DCM, you can fill this field with zeros, replace the DCM, and auto-enroll the new DCM. The new DCM will have the same settings as the replaced unit after you have performed a download to the MLB.

**Module Name** – If desired, you can enter a name for the module. The name entered is displayed on the screen as a part of the DCM identification information.

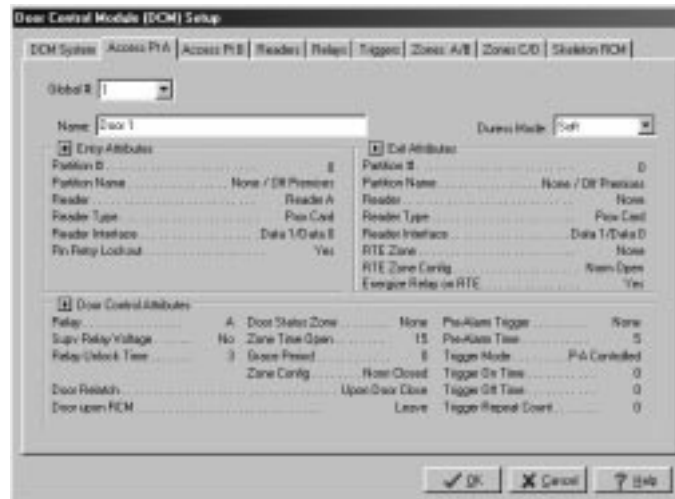
**Module AC Loss Monitor** (Monitor AC Power Flag?) - When this field is enabled, the module notifies the system when it experiences an AC loss condition. An event is logged when the AC power is lost or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

**Module Low Battery Monitor** (Monitor Low Battery Flag?) - When this field is enabled, the module notifies the system when it experiences a low-battery condition. An event is logged when the low-battery condition is detected and/or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

### ***Access Point A/B tabs***

Access point configuration is the specification of the entry and exit controlling devices that are installed at the access point:





Access point configuration also includes information concerning the door locking device and describes the typical timing parameters that govern passage through the access point (such as how long the lock is to operate, how long the door may remain open, etc.). Access point configuration also consists of the access point's name and any other attributes that may need to be specified in order for the access point to operate properly.

From this tab of the DCM Setup screen, three groups of attributes (Entry, Exit, and Door Control) are displayed. On this screen, these attributes CANNOT be edited. This screen acts as a summary screen. Double-click within one of the groups or click on the arrow button to the right of the group name in order to open a screen that will allow you to modify the displayed attributes.

Note that if the Global # for the access point is set to 0, the following fields are not be displayed, as they do not pertain to an unused access point.

**Global Access Point Number** - This field selects the number of this resource from the total number of resources available. Use this drop-down list to select from the allowable values. The system automatically scrolls through only the available numbers.

**Name** - Use this textual field to enter a name for the access point you are defining.

**Duress Mode** - When an individual is being forced to pass through an access point, he can indicate this to the system by substituting a “0” for his last PIN digit.

For example, if the individual's PIN is “1234,” the duress PIN would be “1230.” “0” should be easy to remember, as it the telephone operator’s number. When a duress is initiated, a special message is placed in the event log of the PassPoint system. The system may also initiate a call to a security central station.

The system provides three modes of duress operation: Normal, Soft, and Hard. If the duress mode is set to Soft, entry or egress is granted regardless of the access privileges of the individual. If the individual would not normally be allowed to pass, the duress overrides, and allows the person to pass. In Normal duress mode, the individual is allowed to pass only if his access privileges would normally allow him to pass. In Hard duress mode, access is always be denied. Note that the use of Hard duress may endanger people’s safety and should only be used in the most severe security applications. Use this drop-down list to select the desired mode of operation.

### ***Entry Attributes***

This group displays a summary of all the properties that describe the mode of entry control for this access point. To edit any of these settings, position the cursor on the small arrow button to the right

of Entry Attributes and left-click the mouse; or double click the mouse in the Entry Attributes area. The following menu is displayed where the information can be edited:



**Entry to Partition** - Access point configuration data that describes the access area or partition that an individual enters when he is allowed entry through the access point. Use this drop-down list to select the appropriate Entry to Partition.

**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 the system may examine their access privileges and determine if they should be allowed to pass into the protected area. The term is “entry reader” because in most cases, the device is a card reader at which a cardholder must present his ID card. However, the device may be a keypad at which the individual must enter his assigned Personal Identification Number (PIN code). In some cases, where higher security is required, the entry reader may be a combination keypad/card reader unit.

In the PassPoint system, access points are configured on Door Control Modules (DCMs). Because there are two reader input connections on each DCM, the reader that is being used as the

entry control reader for the access point must be specified. Note that if the installer uses a preset access point configuration, the reader input (A or B) is automatically assigned and does not need to be edited.

**Entry Reader Type** – The type of reader technology or keypad used at the access point. The selections in this field include keypads, different types of ID card readers (Wiegand, proximity, or magnetic stripe), and combination card reader/keypad units. Use this drop-down list to select the appropriate reader type.

**Entry Reader Interface** – The electrical interface style of the reader. All the supported readers that can be used by the system are one of two electrical interface styles: Data1/Data0 (Wiegand style) and Clock & Data. The installer must make the appropriate selection. For most readers other than magnetic stripe card readers, the appropriate selection is usually Data1/Data0. This information is specified by the wiring labels on the card reader or keypad. Select the appropriate Reader Interface method.

**PIN Retry Lockout** - A feature that disables the keypad of an entry reader for a specified period 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 because it slows down the process of trying all possible code combinations. The system logs when PIN Retry Lockout is initiated at an access point. To enable this feature, select *Yes*.

The amount of time for PIN Retry Lockout is set in the Administration dialog box. To reach this dialog box, select *Admin* from the *Config* menu.

## Exit Attributes

This group displays a summary of all the properties that describe the mode of exit control for this Access Point. To edit any of these settings, position the cursor on the small arrow button to the right of Exit Attributes and left-click the mouse or double click the mouse in the Exit Attributes area. The following menu is displayed where the information can be edited:



**Exit to Partition** - Access point configuration data that describes the access area or partition that an individual exits to when he is allowed exit through the access point. If the access point exits out of all controlled areas, this field should be set None/Off Premises. Use this drop-down list to select the appropriate Exit to Partition.

**Exit Reader** - An input device that is installed on the exit side of an access point door. At this device, an individual is required to identify him/herself to the system so that the system may examine their access privileges and determine if he/she should be allowed to pass out of the protected area.

In the PassPoint system, access points can be configured on Door Control Modules (DCMs). As there are two reader input

connections on the DCM, the one that is being used as the exit control reader for the access point must be specified. Note that if the installer uses a preset access point configuration, the reader input (A or B) is automatically assigned, and does not need to be edited.

**Exit Reader Type** - The type of card readers or keypad used for exit at an access point. Use this drop-down list to select the appropriate Reader Type.

**Exit Reader Interface** – The electrical interface style of the exit reader. All the supported readers that can be used by the system are one of two electrical interface styles: Data1/Data0 (Wiegand style) and Clock & Data. For most readers other than magnetic stripe card readers, the appropriate selection is usually Data1/Data0. This information is specified by the wiring labels on the card reader or keypad. Select the appropriate Reader Interface method.

**Request to Exit (RTE) Zone** – The zone that will be used for Request to Exit. In installations where an exit reader is not being employed, it may still be necessary for the system to monitor egresses through an access point and/or unlock the access point. When a DSM is used, if the PassPoint system is not expecting the door to open from the inside when someone leaves, a Request to Exit (RTE or REX) device must be installed.

The RTE device may be a pushbutton on the wall on the protected side of the door or a limited-view passive infrared motion detector focused on the area immediately in front of the door on the protected side. In either case, the RTE device is wired to an input zone on the Door Control Module. When a person requests exit through the access point, the RTE zone is faulted by pressing the button or tripping the motion detector. The PassPoint system unlatches the door locking device, allowing the person to exit through the door. Because the PassPoint system knows that the

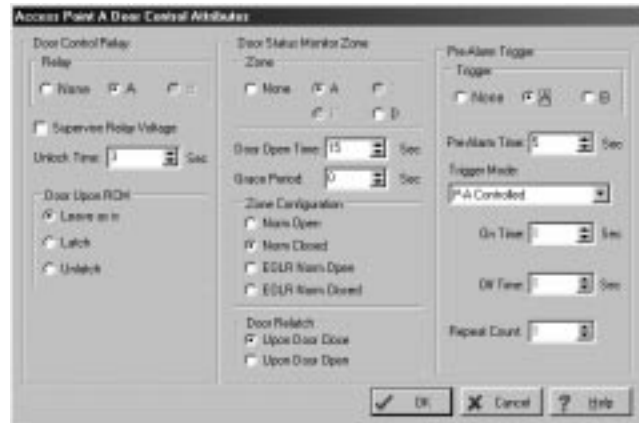
door was supposed to open, it automatically disregards the detection of a door open condition.

The RTE Zone field is used to indicate which of the four DCM input zones (ZONE A thru ZONE D) will be used for this purpose. Note that if the installer chooses a preset access point configuration, this field is automatically filled in by the PassPoint System.

**RTE Zone Configuration** – Zone configuration (normally open, normally closed, or end-of-line-supervised zone configuration) for the RTE device. This setting must correspond with the contact configuration of the RTE device. Additionally, you may allow a relay to be energized on RTE.

### ***Door Control Attributes***

This group is a summary of all the properties that describe the mode of door control for this access point. To edit any of these settings, position the cursor on the small arrow button to the right of Door Control Attributes and left-click the mouse; or double-click the mouse in the Door Control Attributes area. The following menu is displayed where the information can be edited:



**Relay** - An electronic switch that resides on the DCM and is used to control the flow of electricity to the door-locking mechanism. The door control relay is a “form C” dry contact output, which means that it is used to switch a voltage on or off and may be connected as a normally open or a normally closed circuit.

Magnetic door locks are usually connected to the normally closed side of the relay's connections because magnetic locks must be energized in order to hold the door closed. Electronic door strikes are usually connected to the normally open side of the relay's connections, because door strikes usually need to be energized in order to allow the door to open. Note that door strikes are available in Fail Safe (when power is removed, the door may open) or Fail Secure (when power is removed, the door is latched).

Because the locking mechanisms may have life safety implications, note that when a door strike is selected for an application, local fire codes may govern the type and configuration of the locking device chosen, and the appropriate side of the relay's contacts that must be used. As the DCM contains two relay outputs (A or B), this field allows you to select which of the two relays will be used to control this access point's door. If the



installer has chosen a preset access point configuration, the selection of the door control relay is filled in automatically.

**Supervise Relay Voltage** - In situations where a foreign power supply is employed to provide power to the door's locking mechanism, the installer may choose to have the PassPoint system monitor the power supply. This allows the system to notify an administrator when a power supply that is securing a door has failed. Checking this field enables this feature.

If the installer is using the ADEMCO access control's power supply, it may not be necessary to enable this feature, as the output of the power supply may already be supervised by the DCM.

**Unlock Time** - This is the number of seconds the door control relay is to be energized, allowing the door to open. The door locking device should be wired appropriately to the normally open or normally closed circuit side of the door control relay so that during this time, the door may be opened.

**Door Upon RCM** - In the rare event of a Door Control Module losing contact with the rest of the system, you may want a door that has been commanded open (manually or by a timed schedule) to be relatched automatically. This setting allows a setting of "latch," for added exterior door security; "unlatch," for interior doors that would pose a nuisance if they were not able to operate properly, or "leave as is," which leaves the door in its current condition (locked or unlocked). In most cases, the "leave as is" setting will be appropriate. This provides the best security, while allowing individuals with cards (or codes) to pass through the access point if the appropriate Reduced Capability Mode settings have been configured.

**Door Status Monitor Zone** - An input zone on the DCM, which can be wired to a door contact so that the PassPoint system can

determine if an intruder has forced the door open when it should have been closed. This zone can also be used to determine if a door was opened rightfully but was not closed within a specified amount of time.

The Door Status Monitor Zone field is used to indicate which of the four DCM input zones (Zones A thru D) will be used for this purpose. If the installer chooses a preset access point configuration, this field is automatically filled in by the PassPoint System and cannot be edited. Also, if the door can be manually opened from the inside when people leave, it is necessary to install a Request to Exit device so that egresses do not cause Door Forced Open alarms.

**Door Open Time** - The number of seconds that the door is allowed to remain open when access or egress is granted through the access point. If the door remains open longer than the specified time, a Door Open Timeout alarm is generated.

**Grace Period** - The number of seconds, following a DSM Zone Restore, during which a re-opening of the door will not generate a Door Open alarm condition. Instead, it will generate an RTE cycle. An Access Point Door Re-opened event is generated in this case.

This feature is only provided for instances where the DSM may restore prior to the door physically latching closed. This helps to eliminate the occurrence of false alarm conditions. The default setting is zero (0), which disables the Grace Period feature and is the most secure setting. For security purposes, this value should be set to the least possible time period that alleviates the problem.

**Zone Configuration** - This setting allows you to set a normally open, normally closed, or end-of-line-supervised zone

configuration for the DSM device. This setting must correspond with the contact configuration of the DSM device.

**Door Relatch** - When a DSM zone is installed at the door, it is possible for the PassPoint system to determine that the door has closed before the amount of time that it was to remain unlatched. In this case, if the door has not been relatched when it closes, the PassPoint system automatically relatches the door, preventing a late-comer from pushing an unlatched door open. This feature is also called “Anti-Piggybacking.” Most often this option is set to relatch when the door is detected as having closed. The “Upon Door Close” setting should be selected when an electromagnetic door lock is used. The “Upon Door Open” setting can be used at access points that are latched by electronic door strikes.

**Pre-Alarm Trigger** - If a door that employs a DSM is held open longer than the specified Door Open Time, the event history logs a Door Open Timeout alarm. In order to prevent inadvertent Door Open Timeout alarms, a sounder or bell may be installed near the access point to warn someone who is holding a door open that an alarm condition is imminent. This sounder is called a pre-alarm warning device.

When the access point is configured with a pre-alarm device, if the door is still open a preset amount of time before the Door Open Alarm is to occur, the pre-alarm device is energized, giving an audible (or even visible) warning to the person holding the door. Pre-alarm warning devices are usually piezoelectric sounders. P/A devices are driven by one of the two available trigger outputs of the DCM. Each DCM trigger output is an open-collector configured driver, which has a series resistance of 680 Ohms. When energized, trigger outputs sink 15mA of current. If a 12-Volt piezo sounder is used, its positive connection should be wired to a source of 12 Volts (with a ground common to the PassPoint system’s ground) and its negative connection should be connected

to the appropriate trigger output of the DCM. When the P/A warning is in effect, the sounder is energized. As there are two trigger outputs on each DCM, the appropriate one must be chosen (TRIGGER A or TRIGGER B - TRIGA or TRIGB). Because pre-alarm devices are optional, they are never pre-assigned by the PassPoint system and must be selected by the installer.

**Pre-Alarm Time** - The amount of time, in seconds, before the invocation of an access point Door Open alarm at which 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, giving 10 seconds of warning to someone who is holding the door open. The Pre-Alarm Trigger begins to operate 20 seconds after the relay has energized if the door is still open. If the door is still open at the end of the 30 seconds, a Door Open Timeout Alarm Event occurs. The pre-alarm device remains energized (depending upon its mode) until the door is closed, clearing the Door Open Timeout Alarm.

**Trigger Mode** - The pre-alarm trigger output mode can be set to “Controlled,” “One-Shot,” or “Repeating.” A Controlled pre-alarm trigger becomes energized and stays energized until the door is closed. A One-Shot pre-alarm trigger energizes once for the specified On Time, then shuts off. A Repeating pre-alarm trigger output cycles on and off for the specified amount of On Time, Off Time, and for the specified number of Repeat Counts. If the Repeat Count is set to zero, the cycling continues until the door is closed. Note that regardless of the mode, the trigger will turn off as soon as the door is closed.

**On Time** - This is the time, in seconds, that the pre-alarm trigger remains energized if its mode is set as One-Shot. If the mode is set as Repeating, this is the time that makes up the “On” time of a repeating cycle.

**Off Time** - This is the time, in seconds, that the pre-alarm trigger remains de-energized if its mode is set as Repeating. This is the time that makes up the “Off” time of a repeating cycle.

**Repeat Count** - This is the number of repeated On/Off cycles that is expressed by the pre-alarm trigger output. If this number is set to 0, the trigger repeats continuously until the door is closed.

### ***Readers tab***

The readers tab appears as below:



Note that if the Global number is set to 0, the following fields will not be displayed, as they do not pertain to a committed or unused reader.

**Global #** - This field selects the number of this resource from the total number of resources available. Use this drop-down list to select from the available values. The system automatically shows

only the available numbers. Every reader must be given a unique global number.

**Name** - Use this textual field to enter a name for the reader you are defining.

**Type** - This field selects the reader technology type. Use the drop-down list to select the desired type. For the CEK, make sure proximity is chosen in this field.

**Function** - This field selects the function for the uncommitted reader. Setting this field to Enrollment Reader at user terminal x selects this reader to send card numbers to the indicated user terminal when the user is in any field where a card number must be entered. This allows the reader to be used as an enrollment station. Setting this field to Command Reader selects this reader to allow card swipes that can initiate actions within the system. The actions can be programmed through the event/action setting of the system or through the actions assigned to individual cardholders.

**Interface** - The electrical specifications for the reader connected to this interface must be specified in this field. Most units adhere to the Data1/Data0, or Wiegand, wiring standard. Many magnetic stripe card readers conform to the Clock/Data interface method. You must specify the corresponding electrical interface type used by the readers you are installing by selecting the appropriate interface type.

### ***Relay tab***

The relay tab appears as below:



Note that if the Global number is set to 0, the following fields will not be displayed, as they do not pertain to a committed or unused relay.

**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system displays only the available numbers. Every relay used in the system must be given a unique global relay number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the relay you are defining.

**Activation Mode** - You can select from one of three modes:

- **Controlled:** The system or a user can command the relay On or Off.

- **One-Shot:** When commanded by the system or a user, the relay energizes for a specified number of seconds, then de-energizes. [1 - 65535 seconds]
- **Repeating:** When commanded by the system or a user, the relay energizes for a specified number of seconds, then de-energizes for a specified number of seconds. This cycle is repeated for a specified number of times or repeated indefinitely until commanded to stop. [On time = 1-65535 seconds] [Off time = 1-65535 seconds] [Repeat Count = 0 (Continuous) or 1-65535 counts]

**On Time** - This field is active only if you have chosen *One-Shot* or *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the relay should be activated.

**Off Time** - This field is active only if you have chosen *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the relay should be deactivated before it activates again.

**Repeat Count** - This field is active only if you have chosen *Repeating* as the operating mode. Enter the number of times you want the relay to repeat its activate/deactivate cycle. You can choose any number from 0 to 65535. Note that a value of 0 causes the relay to repeat continuously until it is commanded off.

**Supervise Relay Voltage** - Select this field if you want to monitor the voltage going to the relay. If you select this field, the system continuously monitors the relay voltage and displays the status of the relay voltage on a separate status screen.

### ***Triggers tab***

The trigger tab appears as below:





Note that if the Global number is set to 0, the following fields are not displayed, as they do not pertain to a committed or unused trigger.

**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The displays only the available numbers. Every trigger used in the system must be given a unique global trigger number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the trigger you are defining.

**Activation Mode** - You can select from one of three modes:

- **Controlled:** The system or a user can command the trigger On or Off.

- **One-Shot:** When commanded by the system or a user, the trigger energizes for a specified number of seconds, then de-energizes. [1 - 65535 seconds]
- **Repeating:** When commanded by the system or a user, the trigger energizes for a specified number of seconds, then de-energizes for a specified number of seconds. This cycle is repeated for a specified number of times or repeated indefinitely until commanded to stop. [On time = 1-65535 seconds] [Off time = 1-65535 seconds] [Repeat Count = 0 (Continuous) or 1-65535 counts]

**On Time** - This field is active only if you have chosen *One-Shot* or *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the trigger should be actuated.

**Off Time** - This field is active only if you have chosen *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the trigger should be deactivated before it activates again.

**Repeat Count** - This field is active only if you have chosen *Repeating* as the operating mode. Enter the number of times you want the trigger to repeat its activate/deactivate cycle. You can choose any number from 0 to 65535. Note that a value of 0 causes the trigger to repeat continuously until it is commanded off.

## ***Zone tabs***

The dialog box has two Zone tabs. Each tab contains information about two different zones.

The uncommitted zone inputs provided by the PassPoint system are for supplemental functions such as signaling certain conditions. They have not been tested for UL compliance, and as such cannot be used for burglary functions in UL installations.

Both Zone tabs contain similar information. Zones tab A/B appears as below:



Note that if the Global number is set to 0, the following fields are not be displayed, as they do not pertain to an unused zone.

**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system displays only the available numbers. Every zone used in the system must be given a unique global zone number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the zone you are defining.

**Response Type** - Select a response type for the zone. You can select from four different options:


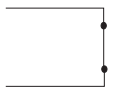
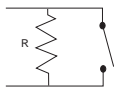
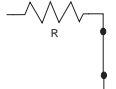
- **No Alarm-Monitored:** This allows the zone to be seen by the system and to trap faults/restores. No Alarm zones are used primarily by event/action relations and system scripts.
- **Perimeter:** Faults/Restores are always recognized on this zone, but can generate an alarm only when the burglary system is armed AWAY or STAY. A perimeter zone restores when the zone returns to normal (zone latches if system is armed).
- **Interior:** Faults/Restores are always recognized on this zone, but can generate an alarm only when the burglary system is armed AWAY. All Interior zones are temporarily ignored for the first 2 minutes after arming AWAY. An Interior zone restores once the zone returns to normal (zone will latch if system armed).
- **24-Hour:** Faults/Restores will always be recognized on this zone. An alarm will be generated whenever this zone is faulted. A 24-Hour zone will restore once the zone returns to normal.

**Configuration** - Select a configuration for the zone. You can select from one of the following:

- Normally Open
- Normally Closed
- EOLR Normally Open

**NOTE:** EOLR zones require ADEMCO's standard 2K-Ohm end-of-line resistors.

- EOLR Normally Closed

Normal Sensor State	ZONE STATES			
	TWO-STATE ZONE (unsupervised)		THREE-STATE ZONE (EOLR supervised)	
	Normally Open (N.O.)	Normally Closed (N.C.)	Normally Open (N.O.)	Normally Closed (N.C.)
0 (short)	FAULT	NORMAL	FAULT	TROUBLE
R	NA	NA	NORMAL	NORMAL
2R	NA	NA	NA	NA
infinite (open)	NORMAL	FAULT	TROUBLE	FAULT
Sensor Connections				

### ***Skeleton RCM tab***

In the rare event that a DCM becomes “disconnected” from the rest of the PassPoint system, the DCM can be told how to operate while it is out of contact. When it is “out of contact,” the DCM is placed in Reduced Capability Mode (RCM). Note that security is not compromised if RCM mode is configured properly. First, each access point can be selected individually to latch, unlatch, or remain as-is when RCM mode is invoked. This allows perimeter doors to be secured while interior or safety zones can be free to open. Cards and PINs can still be used at the card readers and keypads of the DCM in RCM mode. In most cases, skeleton cards or skeleton PINs can be configured and used to unlatch the door, for a single cycle or for extended periods of time. Skeleton cards or PINs can also be used to relatch the door. Skeleton cards are configured by describing the patterns present in the card’s electronic signature. Skeleton PINs are configured by allocating special PIN codes that invoke these features.



For each skeleton card/PIN code, select its function. Each card/PIN can have one of three functions:

- **Grant Access**
- **Unlatch Indefinitely**
- **Latch Indefinitely**

Grant Access operates similarly to a normal access cycle. Unlatch Indefinitely unlatches the door until commanded otherwise. Latch Indefinitely latches the door until commanded otherwise. The latch and unlatch functions can be used by a system administrator who, when the system fails, intends to allow free passage throughout the day until either the end of business, when the latch card (or PIN) is used, or until the system is returned to service.

The type of skeleton code you can enter for an access point depends upon the type of reader you've configured for it. If the access point has only a card reader, for example, you will be able to configure only skeleton cards, not PINs. If you have a

combination unit at the access point, you can configure both type of skeleton codes.



---

**Important:** In this area you are only configuring the function for the skeleton code. The actual card/PIN numbers for skeleton codes are assigned in another area of the program, “System-wide Options,” discussed previously.

---

**Grant PIN of Correct Length?** - Enabling this function disables the use of skeleton PINs. The PIN can be used only at access points that use a keypad for access or egress. Turning on this feature reverts the system to a very low security access point. All that is necessary to gain passage is to enter the correct number of PIN digits. The actual digits used does not matter. Any sequence of digits of the correct length will suffice.





## Chapter

# 10

## *Adding a Card Enrollment Kit*

Adding a Card Enrollment Kit (CEK) allows you to quickly add ID cards to your system. Cards are enrolled into the system by swiping them at a desktop card enrollment station.

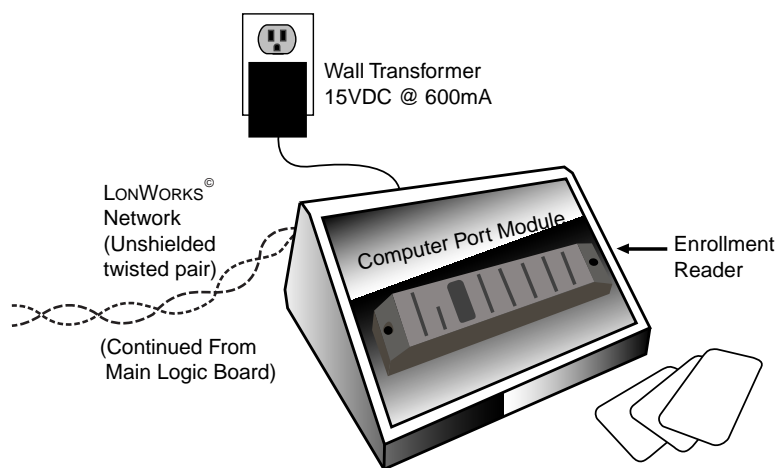
In this chapter you will learn how to:

- **Wire all of the components of the CEK**
- **Activate and set up the CEK**
- **Enroll the CEK into an existing PassPoint system**

## ***Understanding Your Card Enrollment Kit***

The PassPoint Card Enrollment Kit (CEK) is a self-contained system module that can be added to an existing PassPoint installation in order to make the management of cards (including card enrollment) as simple as possible. Essentially, the CEK consists of a desktop enrollment reader (shown below). System administrators can swipe ID cards at this reader to quickly enroll them in the system.

The CEK connects to the PassPoint system like any other system module, using a twisted-pair network connection. It receives power from a 15VDC wall pack transformer.



**CARD ENROLLMENT KIT (CEK)**

**What's in your  
Card Enrollment  
Kit?**

The PassPoint CEK is a kit that includes the following:

- **1 Desktop case, containing:**  
Computer Port Module (PTCPM)  
Proximity reader, for card enrollment (PTPROX)
- **1 twisted-pair network cable connector**
- **1 plug-in transformer**

## ***Installing the CEK***

There are seven steps to install and enroll the CEK into an existing PassPoint system. Follow each of the steps below and refer to the wiring diagram provided.

### ***Step 1 - Choose a location for the CEK***

The CEK is essentially a stand-alone unit; that is, it can be placed on a desk or any other convenient work area. However, the CEK must be located near the system computer, as this is where card enrollment takes place. The administrator will need easy access to both the computer and the CEK when enrolling cards.

### ***Step 2 - Connect the CEK to the system***

Connecting the CEK to the system simply means wiring the CEK into the existing twisted-pair network. To do so, follow the steps below and refer to the connections diagram provided:

1. **Connect the “plug” end of the network cable into the socket of the enrollment reader labeled *NETWORK*.**

The twisted-pair network cable supplied with the CEK has two ends. One end contains a two-prong plug. This is the end that gets connected into the enrollment reader.

2. **Connect the two leads on the other end of the network cable to terminals 15 and 16 of the MLB.**

Either lead can be connected to either MLB terminal.

---



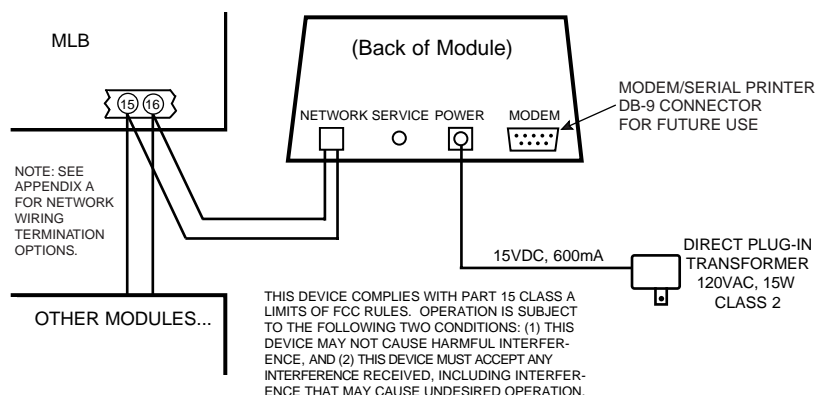
See Appendix A for wiring termination options.

---

### ***Step 3 - Connect the power transformer and activate the system***

The CEK comes with a wall-pack power transformer to be connected between the enrollment reader and a power source.

1. **Connect the applicable end of the power lead into the socket of the enrollment reader labeled *POWER*.**
2. **Plug the transformer into a suitable power source and activate the system.**



#### CARD ENROLLMENT KIT CONNECTIONS

### Step 4 - Add and set up the CEK

Now that the CEK is powered up, you must add the new module (CPM) to your existing installation. To add and set up the new CPM, follow the procedure below:

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

The Installer Configuration dialog box appears:

Use the Installer Configuration dialog box to view/modify system components and to set various system options.

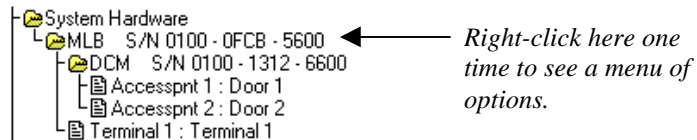


The Installer Configuration dialog box lists all of the components of the system. Here is where you add new system modules.



Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

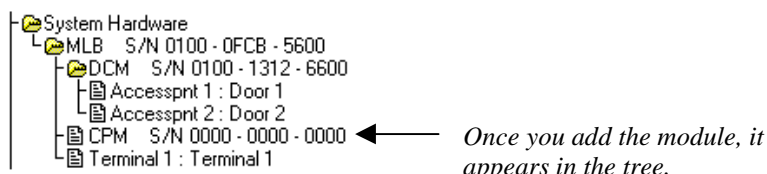
## 2. **Right-click on the MLB once.**



This will bring up a menu of options.

## 3. **From the menu, select *Add CPM*.**

The tree in the Installer Configuration dialog box now shows your new CPM:



Now you must enroll the CPM into the PassPoint system so that the system recognizes the device and all its configuration settings. Enrolling the CPM is covered in the next step.

## Step 5 - Auto enroll the CPM

Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because these modules have serial numbers that contain only zeros. For instance, look at the CPM you have just added. It has a serial number that contains only zeros, no other digits. That means it has not been enrolled, and is not truly part of the system yet.

To enroll the CPM you just added, follow the procedure below:

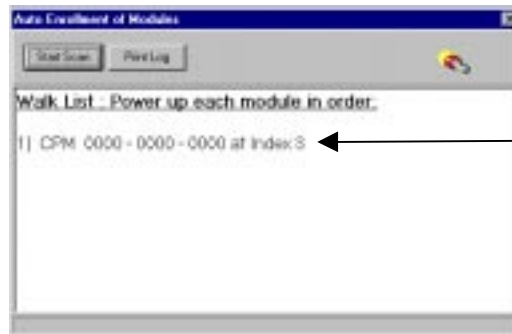
1. **Click the Auto Enroll button on the Installer Configuration dialog box.**

Refer to the diagram below for the location of the Auto Enroll button:



Auto Enroll  
button

Clicking this button brings up the Auto Enroll dialog box, shown below:



System recognizes  
that a CPM needs  
to be enrolled.

The enrollment process is all done **automatically** once you click *Start Scan*. The entire process takes no more than a few moments.

The procedures required to enroll a single module are different than those required to enroll multiple modules. If enrolling a single module, perform the steps listed under 2a below. If enrolling more than one module, perform the steps under 2b below.

### 2a. Enrolling a Single Module.

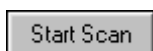
To enroll a single module into your PassPoint system, proceed as follows:





Never power down the MLB while the system is enrolling a module.

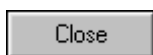
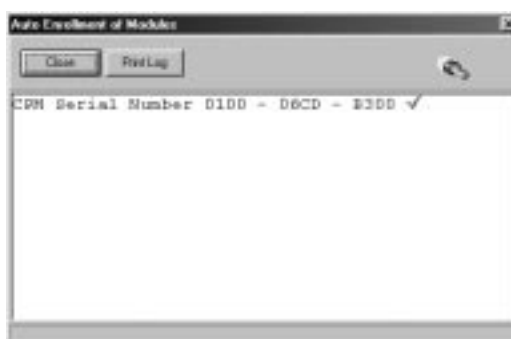
---



**(1) Click the *Start Scan* button.**

The system searches for the module. When the module is found, the system blinks the yellow service LED on the module, presents a screen message indicating that the module has been enrolled, and stops scanning for modules.

After the system has enrolled the module, a screen is presented that shows the module (with serial number) that has been enrolled.



**(2) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

**2b. Enrolling Multiple Modules.**

The Auto Enroll dialog box should already be on your screen, and should look something like this when enrolling multiple modules:




If the modules are powered up before the enrollment process or powered up in the wrong order, they will be enrolled incorrectly. Never power down the MLB during the enrollment process.



To enroll multiple modules into your PassPoint system, the modules must be powered up in the order that they are listed on the screen. To enroll the modules, proceed as follows:

- (1) **Click the *Print Log* button.** A “walk list” of all the modules waiting to be enrolled is printed.
- (2) **Verify the power is applied to the first module listed only.**

**NOTE:** You must power up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered up.

A rectangular button with a black border and the text "Start Scan" in a sans-serif font.

**(3) Click the *Start Scan* button.**

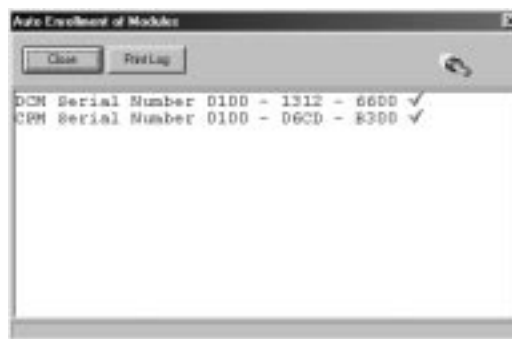
The system searches for the first module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. Next, a message will be displayed indicating that the system is polling for the next module in the “walk list.”

**(4) Apply power to the next module in the list.**

The system searches for the next module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. If additional modules are in the list, a message will be displayed indicating that the system is polling for the next module.”

**(5) Repeat the application of power to the modules, one at a time, until all modules have been enrolled.**

When the system has enrolled the last module in the list, the screen shows a listing of modules (with serial numbers) that have been enrolled.





**(6) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

## ***Step 6 - Configure the reader***

In order for the CEK's reader to function, it must be configured. You need to tell it how to function so that the system will know how to use it. This same procedure may be used to edit information on a CEK that was already configured.

To configure the CEK reader:

**1. In the Installer Configuration dialog box, right-click on the CPM.**

A sub-menu of choices appears.

**2. Select *Properties* from the sub-menu.**

Selecting *Properties* calls up a dialog box for the module. This dialog box contains tabs and fields of information describing how the module functions. Each field can be modified to tailor the functioning of the module.

**3. Click the *Reader* tab.**

**4. Fill in the fields of the Reader tab as applicable.**

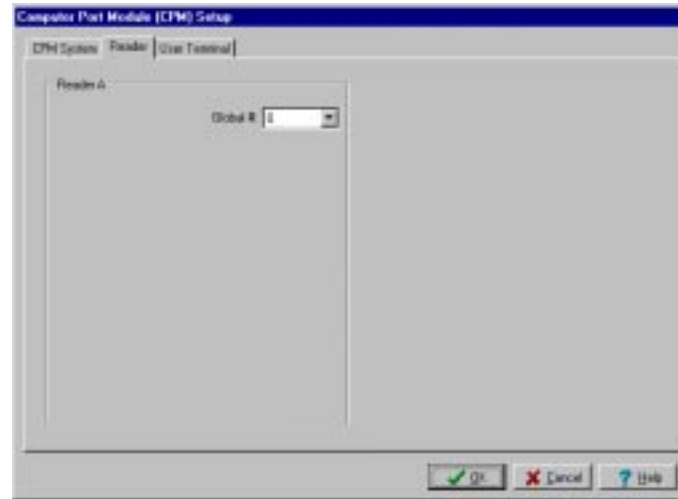
Refer to the following section for a description of each field.

**5. When you are finished, click *OK*.**

Once you click *OK*, you can download the database to save your changes. Refer to the section of this chapter titled "Download the Database" for information on performing this step.

## **Reader tab**

The reader tab appears as below:



**Global #** - This field selects the number of this resource from the total number of resources available. While this number is 0, no other fields will be displayed. Use the drop-down list to select from the available values. The system displays only the available numbers. Every reader must be given a unique global number. When a global number has been selected, the reader tab appears as shown below:



**Name** - Use this textual field to enter a name for the reader you are defining.

**Type** - This field selects the reader technology type. Use the drop-down list to select the desired type. For the CEK, make sure proximity is chosen in this field.

**Function** - This field selects the function for the uncommitted reader. Setting this field to Enrollment Reader at User Terminal x selects this reader to send card numbers to the indicated User Terminal when the user is in any field where a card number must be entered. This allows the reader to be used as an Enrollment Station. Setting this field to Command Reader selects this reader to allow card swipes that can initiate actions within the system. The actions can be programmed through the event/action setting of the system or through the actions assigned to individual cardholders.

**Interface** - The electrical specifications for the reader connected to this interface must be specified in this field. Most units adhere to

the Data1/Data0, or Wiegand, wiring standard. Many magnetic stripe card readers conform to the Clock/Data interface method. You must specify the corresponding electrical interface type used by the readers you are installing by selecting the appropriate interface type.

### ***User Terminal tab***

Selections under this tab are not currently used and are reserved for future product enhancements.

## ***Step 7 - Download the database***

The last step in getting your CEK operational is to download the database.



---

Remember, the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your computer, these changes are not automatically made to the database on the MLB. They are kept in a temporary storage area on your computer until you download them to your MLB database. Any changes made on the computer must be downloaded to the database in order for them to take effect.

---

### **1. Close the Installer Configuration dialog box.**

At close, the system automatically asks you if you want to download the database:



### **2. Click Yes.**

The Download dialog box appears:



At the top of the dialog box is the account number you will be downloading. Make certain that you are downloading to the correct account. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes are automatically checked for you according to the system options you have changed. If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

### 3. Click *Start*.

The database download now proceeds. The status bar at the bottom of the dialog box tracks the progress of the download. This may take several minutes, depending on the size of your database.



## Chapter

# 11

## *Adding a VISTA Gateway Module*

Adding a VISTA Gateway Module (VGM) provides an interface between the PassPoint ACS and an ADEMCO VISTA Fire/Burglary Alarm System (VISTA FBS). To determine if your VISTA Fire/Burglary Alarm System is compatible with the VGM, consult your Alarm System Manuals.

In this chapter you will learn how to:

- **Wire the VGM**
- **Activate and set up the VGM**
- **Enroll the VGM into an existing PassPoint system**

## ***Understanding Your VISTA Gateway Module***

When the VGM is used to link the PassPoint ACS and VISTA FBS, the VISTA FBS provides a dialer function for the PassPoint ACS. Dialer events are sent through the VGM to the VISTA FBS panel, which actually does the dialing. The VISTA FBS panel supports all of the access control-related Contact ID event codes. In addition, linking these two systems together allows the behavior of each subsystem to change based upon status changes or occurring events. The following lists some of the features that are available when using the VGM to interface between the PassPoint ACS and VISTA FBS:

- **VISTA FBS RF devices, such as RF button remotes, transmitters, wireless keypads, and motion detectors can control access functions.**
- **The multitude of zones present in the VISTA FBS expands the capability of the PassPoint ACS.**
- **Card users can be programmed to disarm or arm both systems.**
- **The access point modes of operation (PROTECT, BYPASS, or LOCKED) can be controlled via the VISTA FBS keypad.**
- **A fire alarm detected in the VISTA FBS can be programmed via the PassPoint system to cause the access points to be bypassed, enabling fire department personnel to enter the building.**
- **An access grant can be programmed to disarm both the VISTA FBS and PassPoint systems while turning on the lights.**

- **An egress grant can be programmed to arm both the VISTA FBS and PassPoint systems and turn off the lights.**
- **Systems already installed with a VISTA FBS system or PassPoint system can be upgraded easily by installing the VGM.**

## ***Installing the VGM***

There are seven steps to install and enroll the VGM into an existing PassPoint system. Follow each of the steps below and refer the wiring diagram provided.

### ***Step 1 - Mount the VGM***

The VGM must be located near the VISTA FBS panel. The VGM should be mounted on a sturdy wall using fasteners or anchors (not supplied).

**Using anchors or fasteners, mount the VGM to the wall.**

---



When mounting the VGM, be very careful not to jar the module's PC board.

---

## Step 2 - Connect the VGM

Connecting the VGM actually involves the following steps:

- **Connecting the VGM to the VISTA FBS (and external power supply, if used)**
- **Connecting the VGM to the PassPoint ACS MLB**



---

**Do not apply power** to the system until all cables, including power connections, are attached. Make sure that the component supplying power to the VGM, whether a separate power supply or another module, is not powered while connecting to the VGM. After all connections are complete, power may be applied to the system.

---

### **Connecting the VGM to the MLB**

1. **Remove all power (wall and battery) to the PassPoint ACS and VISTA FBS.**
2. **Connect two network connection leads between the MLB and VGM.**

Connect one lead between terminal 7 of the VGM and terminal 16 of the MLB.

Connect the other lead between terminal 8 of the VGM and terminal 15 of the MLB.



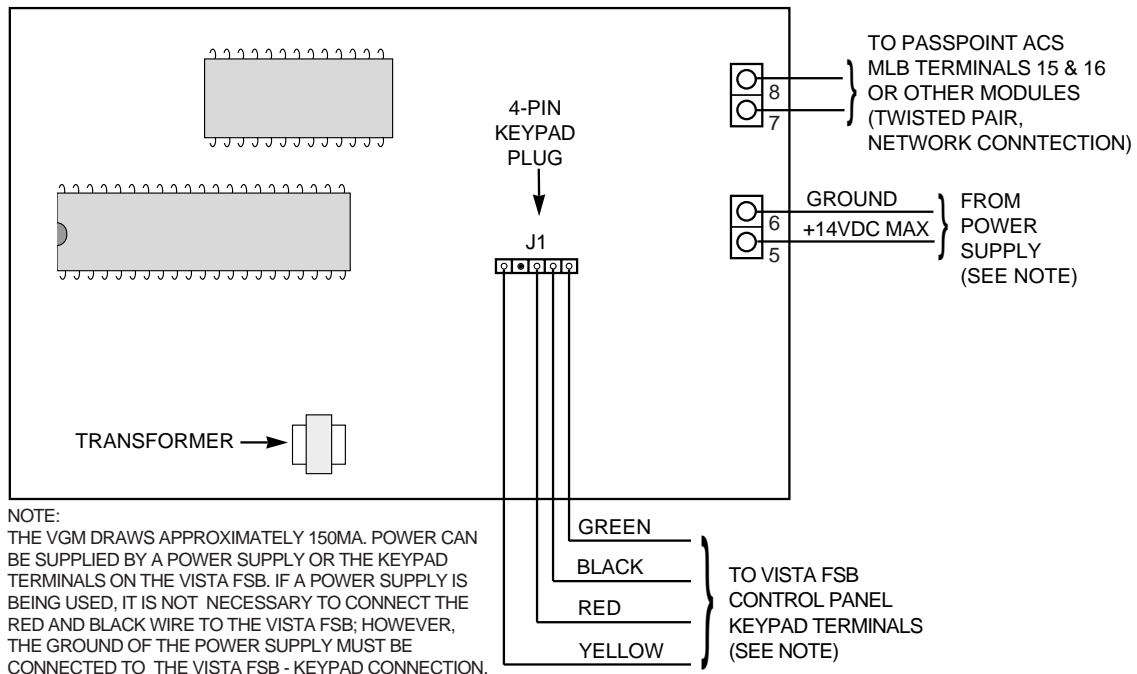
---

Use twisted-pair wiring for these connections. Also, use proper termination for the modules. Refer to Appendix A for details.

---

**Connecting the VGM to the VISTA FBS**

1. Connect the four-wire keypad cable (supplied) to J1 on the VGM.
2. Connect the Green and Yellow wires in the cable to the VISTA FBS keypad terminals.
3. If you are using the VISTA FBS to supply VGM power (recommended), connect the Red and Black wires in the cable to the VISTA FBS keypad terminals. If you are not using the VISTA FBS for VGM power, attach the + input of the power supply to VGM terminal 5 and the ground side of the power supply to VGM terminal 6 and the VISTA FBS keypad ground (Black).
4. Apply power to the PassPoint ACS and VISTA FBS.





See Appendix A for wiring termination options.

### Step 3 - Add and set up the VGM

Now that the VGM is powered up, you must add the new module to your existing installation. To add and set up the VGM, follow the procedure below:

#### 1. From the *Config* menu, select *Hardware*.

The Installer Configuration dialog box appears:

Use the Installer Configuration dialog box to view/modify system components and to set various system options.

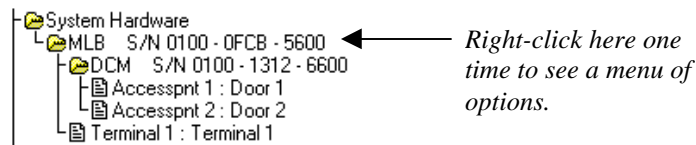


The Installer Configuration dialog box lists all of the components of the system. Here is where you add new system modules.



Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

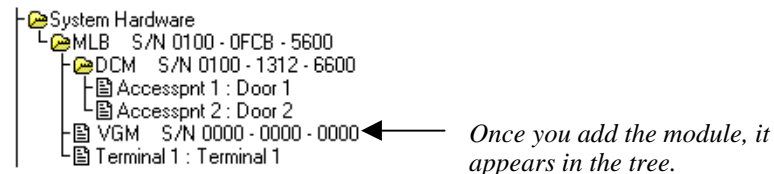
## 2. **Right-click on the MLB once.**



This will bring up a menu of options.

## 3. **From the menu, select *Add VGM*.**

The tree in the Installer Configuration dialog box now shows your new VGM:



Now you must enroll the VGM into the PassPoint system so that the system recognizes the device and all its configuration settings. Enrolling the VGM is covered in the next step.

## **Step 4 - Auto enroll the VGM**

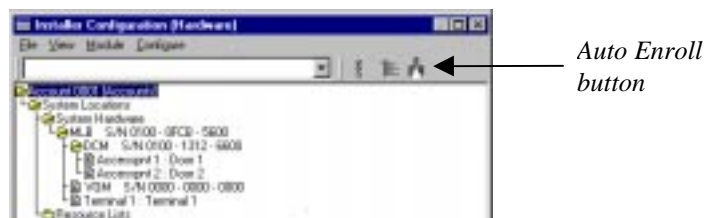
Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because these modules have serial numbers that contain only zeros. For instance, look at the VGM you have just added. It has a serial number that contains only zeros, no other digits. That means that it has not been enrolled, and is not truly part of the system yet.

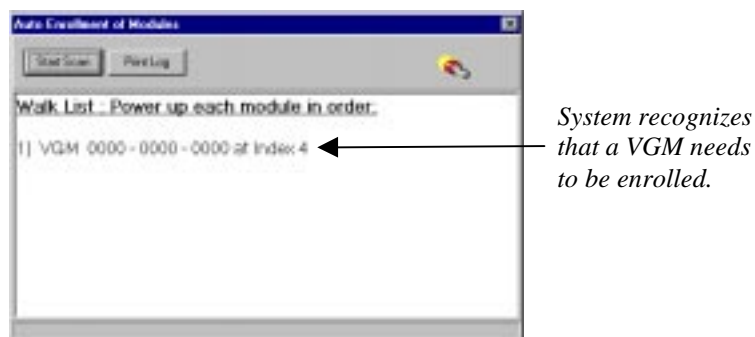
To enroll the VGM you just added, follow the procedure below:

**1. Click the Auto Enroll button on the Installer Configuration dialog box.**

Refer to the diagram below for the location of the Auto Enroll button:



Clicking this button brings up the Auto Enroll dialog box, shown below:





The enrollment process is all done **automatically** once you click *Start Scan*. The entire process takes no more than a few moments.

The procedures required to enroll a single module are different than those required to enroll multiple modules. If enrolling a single module, perform the steps listed under 2a below. If enrolling more than one module, perform the steps under 2b below.

### 2a. Enrolling a Single Module.

To enroll a single module into your PassPoint system, proceed as follows:

---



Never power down the MLB while the system is enrolling a module.

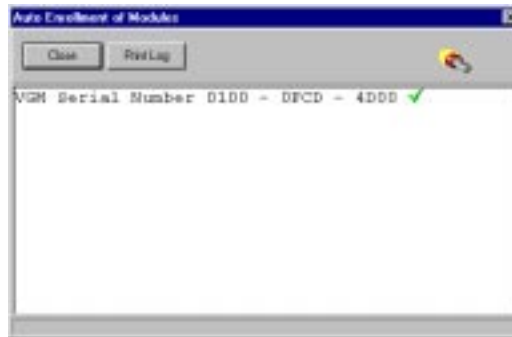
---



#### (1) Click the *Start Scan* button.

The system searches for the module. When the module is found, the system blinks the yellow service LED on the module, presents a screen message indicating that the module has been enrolled, and stops scanning for modules.

After the system has enrolled the module, a screen is presented that shows the module (with serial number) that has been enrolled.

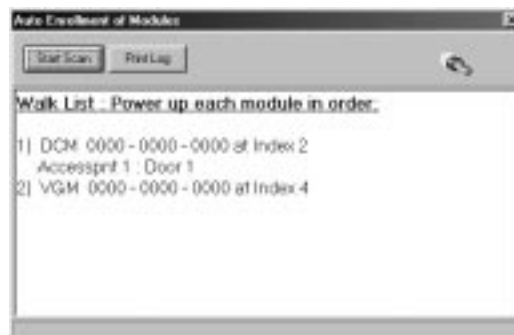


**(2) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

**2b. Enrolling Multiple Modules.**

The Auto Enroll dialog box should already be on your screen, and should look something like this when enrolling multiple modules:



If the modules are powered up before the enrollment process or powered up in the wrong order, they will be enrolled incorrectly. Never power down the MLB during the enrollment process.

To enroll multiple modules into your PassPoint system, the modules must be powered up in the order that they are listed on the screen. To enroll the modules, proceed as follows:

A rectangular button with a thin black border and a light gray background. The text "Print Log" is centered in a black, sans-serif font.

- (1) **Click the *Print Log* button.** A “walk list” of all the modules waiting to be enrolled is printed.

- (2) **Verify the power is applied to the first module listed only.**

**NOTE:** You must power up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered up.

A rectangular button with a thin black border and a light gray background. The text "Start Scan" is centered in a black, sans-serif font.

- (3) **Click the *Start Scan* button.**

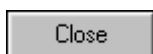
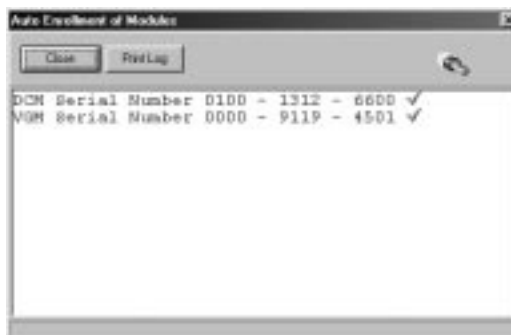
The system searches for the first module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. Next, a message will be displayed indicating that the system is polling for the next module in the “walk list.”

- (4) **Apply power to the next module in the list.**

The system searches for the next module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. If additional modules are in the list, a message will be displayed indicating that the system is polling for the next module.”

- (5) **Repeat the application of power to the modules, one at a time, until all modules have been enrolled.**

When the system has enrolled the last module in the list, the screen shows a listing of modules (with serial numbers) that have been enrolled.



**(6) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

**3. Click the *Close* button.**

The VGM serial number is added to the VGM listing in the Installer Configuration (Hardware) screen.

## ***Step 5 – Enable the VGM in the VISTA FBS***

The VGM must be enabled in the VISTA FBS so that it will also recognize the VGM. Refer to your VISTA FBS *Installation and Setup Guide* for procedures on enabling the VGM. When you enable the VGM in the VISTA FBS, note the device address assigned to the VGM. This address is needed to configure the VGM in the PassPoint ACS.

## Step 6 - Configure the VGM

In order for the VGM to function, it must be configured. Configuration of the VGM consists of defining Test Report Schedules, setting the VGM to act as an interface, and defining controls for PassPoint Zones. This same procedure may be used to edit information on a VGM that was already configured.

To configure the VGM:

1. **In the Installer Configuration dialog box, right-click on the VGM.**

A sub-menu of choices appears.



2. **Select *Properties* from the sub-menu.**

Selecting *Properties* calls up a dialog box for the module. This dialog box contains tabs and fields of information describing how the module functions. Each field can be modified to tailor the functioning of the module to the requirements of the installation.

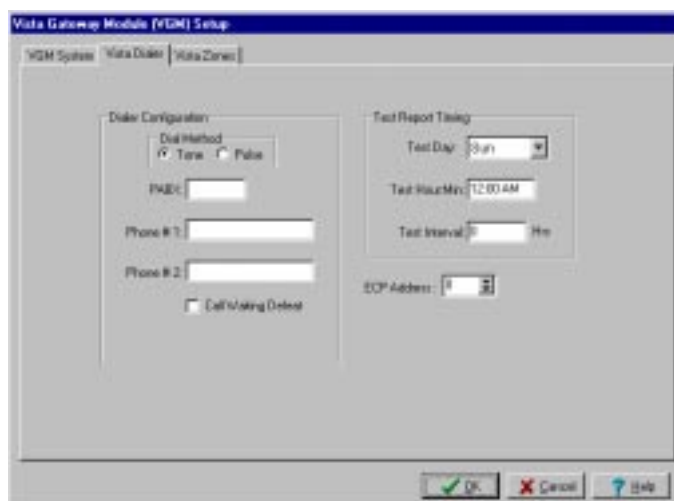


### ***Defining Test Report Schedules and VGM Interface***

To configure the Test Report Schedules and define the VGM as an interface between the PassPoint ACS and VISTA FBS, proceed as follows:

- 1. Select the *Vista Dialer* tab on the screen.**

The Dialer Configuration screen shown below is displayed:



**2. Configure the VGM Test Report Schedules and set the VGM to act as an interface between the PassPoint ACS and VISTA FBS by completing the entries on the screen.**

The subfields on the screen allow definition of the configuration as follows:

**Dialer Configuration** - All subfields in this area (Dial Method, PABX, Phone # 1, Phone # 2, and Call Waiting Defeat) may be left blank. Dialing functions will be performed by the VISTA FBS. Note that this area will not be visible after the ECP address is set.

**Test Report Timing** - This field controls when PassPoint test reports are sent to the central station. The following subfields control test report timing:

**Test Day** - Select the day of the week to start sending test reports.

**Test Hour:Min** - Choose the time of day that is to be used to initiate the test-reporting interval.

**Test Interval** - Enter the number of hours between test reports. Reports will not be generated if this field is set to zero.

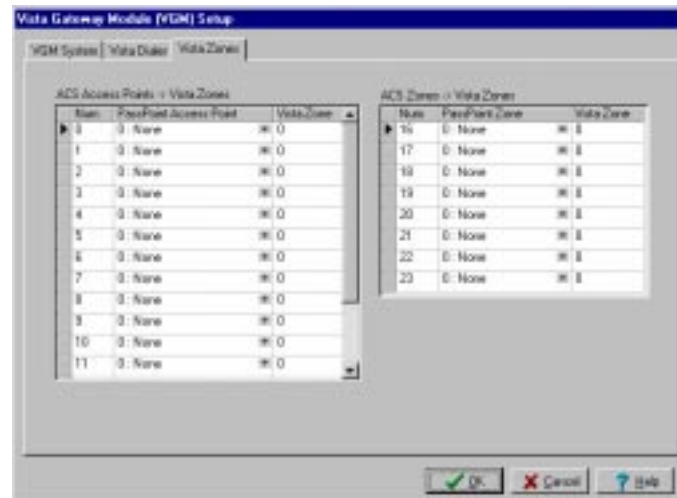
**ECP Address** - Set this field to match the device address assigned the VGM in the VISTA FBS.



The ECP address must be set to a non-zero value and match the address that was programmed in the VISTA FBS.

## Defining VISTA Zones

Select the **Vista Zones** tab on the screen. The ACS Access Points to Vista Zones/ACS Zones to Vista Zones Configuration screen shown below will be displayed:





### **Defining PassPoint ACS Access Points as VISTA FBS Zones**

The state of up to 16 PassPoint ACS access points can be reported to the VISTA FBS, where they also can be treated as hardwired VISTA FBS zones. This allows one door contact to be installed, yet allow the PassPoint ACS door logic and a VISTA FBS alarm zone to be configured at the door. The access point will be mirrored into the VISTA FBS panel without having to run redundant wiring. When programmed, PassPoint ACS access point door-open alarms (and door-open-time alarms), restores, and troubles are transmitted from the PassPoint ACS to the VISTA FBS. Note that processing of events on both systems can still happen independently. You can still use event/action relationships on PassPoint ACS for access point alarms and restores in addition to initiating alarms in the VISTA FBS based upon its arming modes. Another benefit of defining access points as VISTA FBS zones is that just as a VISTA FBS alarm panel prevents arming with zone faults, a bypassed (unlatched) door that is propped open prevents the VISTA FBS panel from arming, as well.

Reports for access point status changes are sent to the VISTA FBS as listed below:

Status	ACCESS POINT MODE	
	Lock, Protect, and Exit Only	Bypassed
Fault	Immediately on Forced Immediately on Door Open Timeout	Immediately on Door Opening
Fault Restore	Immediately when Forced corrects Immediately when Door Open Timeout corrects	Immediately on Door Closing
Trouble	Immediately when it occurs	Immediately when it occurs
Trouble Restore	Immediately when it occurs	Immediately when it occurs

When a card is swiped at a Locked, Protected ,or Exit Only access point or if a door opening is performed within the programmed door timing parameters, the VISTA FBS never “sees” a fault and restore. If the door operation results in a door forced alarm or a door open timeout alarm, the VISTA FBS is notified of the fault. The zone reporting status for a bypassed access point allows a bypassed access point that is propped open to prevent the VISTA FBS from arming due to the fault condition.

---



Shunted Access Points or ACS Zones will NOT cause Fault, Fault Restore, Trouble, or Trouble Restore status to be sent to the VISTA FBS, causing a lack of protection.

---

To configure the VGM to report PassPoint ACS access points as VISTA FBS zones, proceed as follows:

The access points being defined must already exist in PassPoint before you perform the following procedure.

- 1. In the ACS Access Point -> Vista Zones area of the screen, position the cursor on the down (▼) button in the PassPoint Access Point column for the number (0-15) being defined. Left-click the mouse, position the cursor on the desired access point in the list that is displayed, and left-click the mouse again.**
- 2. Move the cursor to the Vista Zone area and enter the number of the zone in the VISTA FBS that will be assigned to this PassPoint access point.**
- 3. Repeat steps 1 and 2 for each access point (up to 16) that is to be reported to the VISTA FBS.**

4. **Record the PassPoint Num column and corresponding VISTA FBS zone number. You will need this information to program the VISTA FBS.**
5. **Referring to your VISTA FBS Installation and Setup Guide, program the VISTA FBS zone that corresponds to the Vista Zone assignment defined in the Vista Zone column of the VGM screen as a type 10 (ACS). Then, enter the VGM zone number from the Num column of the VGM screen (0-15). Repeat this operation for each PassPoint access point being reported to the VISTA FBS.**

### ***Defining PassPoint ACS Zones as VISTA FBS Zones***

In order to obtain the wiring benefits of PassPoint's Echelon Lonworks based network, up to eight sensors that have been hardwired into a PassPoint module's zones can be mapped into the VISTA alarm panel's zones. This allows a protective zone that may be in close proximity to a PassPoint module to be treated as if it were a VISTA FBS hardwired zone without having to run redundant wiring. In order to do this, PassPoint must be configured to report zone status changes to the VGM on the zones that need to be transferred to the VISTA panel. Zone faults, restores, and troubles are sent as they occur.

To configure the VGM to report PassPoint ACS zones as VISTA FBS zones, proceed as follows:

The zones being defined must already be configured in the MLB, DCM(s), or ZIM(s) before you perform the following procedure.



Shunted ACS Zones will NOT cause Fault, Fault Restore, Trouble, or Trouble Restore status to be sent to the VISTA FBS, causing a lack of protection.

1. In the ACS Zones -> Vista Zones area of the screen, position the cursor on the down (▼) button in the PassPoint Zone column for the number (16-23) being defined. Left-click the mouse, position the cursor on the desired zone in the list that is displayed and left-click the mouse again.
  2. Move the cursor to the Vista Zone area and enter the number of the zone in the VISTA FBS that will be assigned to this PassPoint Zone.
- 



The VISTA zone number must be a non-zero value for a properly mapped zone.

---

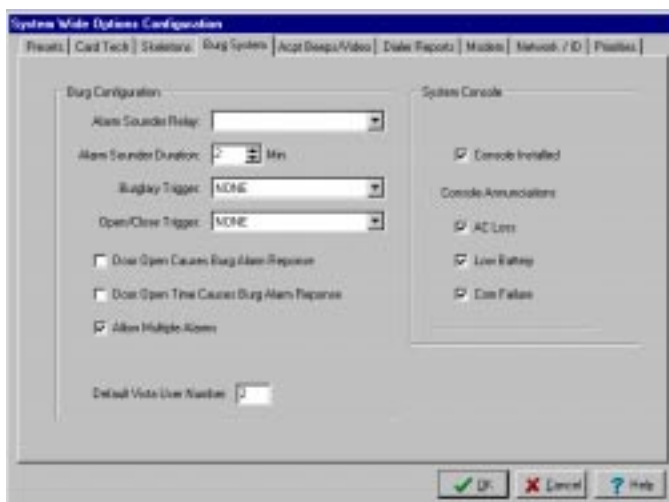
3. Repeat steps 1 and 2 for each zone (up to 8) that is to be reported to the VISTA FBS.
4. Record the PassPoint Num column and corresponding VISTA FBS zone number. You will need this information to program the VISTA FBS.
5. Referring to your VISTA FBS Installation and Setup Guide, program the VISTA FBS zone that corresponds to the Vista Zone assignment defined in the Vista Zone column of the VGM screen as a type 10 (ACS). Then, enter the VGM zone number from the Num column of the VGM screen (16-23). Repeat this operation for each PassPoint zone being reported to the VISTA FBS.

### ***Defining the Default VISTA FBS User Number***

All actions on a PassPoint ACS connected to a VISTA FBS alarm panel get logged to the VISTA FBS event history log. Because all actions are logged, any action that the PassPoint ACS system

initiates on the VISTA FBS panel should map to a VISTA FBS user number. The default VISTA user number defined in this field will be associated with any VISTA action that is induced by the PassPoint ACS system. To define the default VISTA FBS user number, proceed as follows:

1. Select **Configure** from the **Installer Configuration** menu bar.
2. Select **System Wide Options** from the **Configure** menu list. The system wide options configuration screen appears.
3. Select the **Burg System** tab and a screen similar to that shown below appears.



4. The **Default Vista User Number** field displays a number 2 (default value) if the field has never been modified. You may choose to keep the number 2 if it is acceptable, or enter a new number. When the desired **Default Vista User Number** is displayed, click on the **OK** button.

When programming your VISTA FBS, it is important to remember the following items:

- The User Number defined in this screen must be enabled in the VISTA FBS for access to the Partition/Zone that the PassPoint ACS is reporting to.
- If using the PassPoint ACS to open or close a VISTA FBS partition, the User must have open/close capability in the VISTA FBS.
- If using a card in the PassPoint ACS to initiate an event that results in a VISTA FBS related action, the VISTA user number must be enabled in the VISTA FBS with the rights to perform the action. When the action is reported to a central station, the VISTA user number will be reported as the initiator of the action.

## ***Step 7 - Download the database***

The last step in getting your VGM operational is to download the database.



---

Remember, the PassPoint system database resides on the MLB. Here is where all of your system configuration data is stored. However, when you make changes on your computer, these changes are not automatically made to the database on the MLB. They are kept in a temporary storage area on your computer until you download them to your MLB database. Any changes made on the computer must be downloaded to the database in order for them to take effect.

---

- 1. Close the Installer Configuration dialog box.**

At close, the system will automatically ask you if you want to download the database:



**2. Click Yes.**

The Download dialog box appears:



At the top of the dialog box is the account number you will be downloading. Make certain that you are downloading to the correct account. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes are automatically checked for you according to the system options you have changed. If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

**3. Click Start.**



---

The database download proceeds. The status bar at the bottom of the dialog box tracks the progress of the download. This may take several minutes, depending on the size of your database.



## Chapter

# 12

## *Adding System Modules*

System modules are stand-alone modules that are not part of a PassPoint Kit. Individual modules can be added to expand your PassPoint system.

In this chapter you will learn:

- **What types of modules can be added to your system**
- **How to add and enroll individual system modules**
- **How to configure each type of system module**

## ***Understanding System Modules***

Up to this point, you have seen how to add kits to your PassPoint system in order to expand its functionality. You know also that kits contain modules, such as MLBs and DCMs. However, the PassPoint system can be expanded without kits, by adding individual modules directly to the installation. For instance, if you want to add a DCM to the system, you can do so without adding an entire Door Expansion Kit. Adding modules separately allows you greater flexibility when expanding your system.

There are five types of modules that can be added to your system. They are:

- **Door Control Module (DCM)**
- **Quad Relay Module (QRM)**
- **Computer Port Module (CPM)**
- **VISTA Gateway Module (VGM)**
- **Zone Input Module (ZIM)**



---

If you need additional power when adding modules, a power supply (PTCANPOWER) is available. This power supply is the same as the PTDPSU except that it is mounted in a can that has room to mount two additional modules.

---

### ***How do you add a module to a system?***

Essentially, there are four steps to adding an individual system module to an existing PassPoint system. These four steps apply to each type of module, and are:

Step 1 - Install the module

Step 2 - Enroll the module

Step 3 - Configure the module

Step 4 - Download the database

## ***Installing Modules***

Each system module purchased comes with its own installation instructions. These instructions detail all the steps needed to get the module installed in an existing PassPoint system. Included in these instructions are wiring information, mounting procedures, etc. Refer to the documentation accompanying your system module for instructions on performing this step.

## ***Adding and Enrolling Modules***

Once the module has been physically installed, it must be added to the system and enrolled so that the system knows that it's there and can recognize it. To add the new module to the system, follow the procedure below:

### ***Adding a module***

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

The Installer Configuration dialog box appears:

Use the Installer Configuration dialog box to view/modify system components and to set various system options.



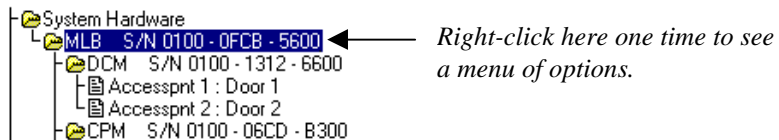
The Installer Configuration dialog box lists all of the components of the system. Here is where you add new system modules.



Once you make changes in this screen, the changes must be downloaded to the system database in order for them to take effect.

## 2. **Right-click on the MLB once.**

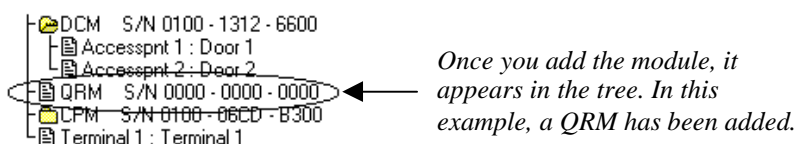
This brings up a menu of options.



## 3. **From the menu, select Add QRM (or DCM, CPM, VGM, or ZIM).**

**NOTE:** A menu choice for a PPM is also provided. This choice is not currently used. The choice is reserved for future product enhancement.

The tree in the Installer Configuration dialog box now shows your new module:



Now you must enroll the module into the PassPoint system so that the system recognizes the device and all its configuration settings. Enrolling the module is covered in the next step.

### ***Enrolling a module***

Whenever a new module is added to the system, it must be enrolled. Enrolling simply informs the system database that a new system module is present.

When you enroll a system module, the system searches for any modules connected to it that have not been enrolled. It knows which modules are not enrolled because these modules have serial numbers that contain only zeros.

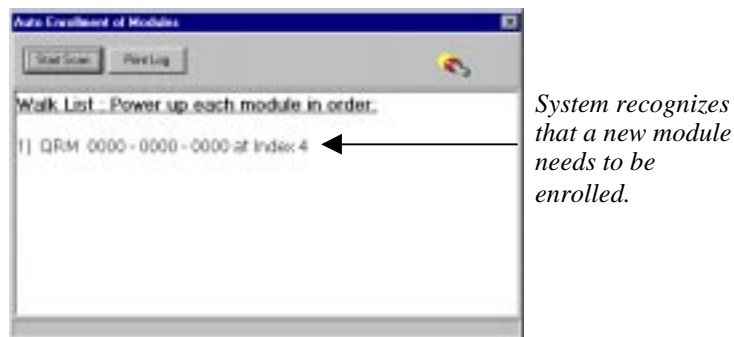
To enroll the module you just added, follow the procedure below:

- 1. Click the Auto Enroll button on the Installer Configuration dialog box.**

Refer to the diagram below for the location of the Auto Enroll button:



Clicking this button brings up the Auto Enroll dialog box, shown below:



The enrollment process is all done **automatically** once you click *Start Scan*. The entire process takes no more than a few moments.

The procedures required to enroll a single module are different than those required to enroll multiple modules. If enrolling a single module, perform the steps listed under 2a below. If enrolling more than one module, perform the steps under 2b below.


## 2a. Enrolling a Single Module.

To enroll a single module into your PassPoint system, proceed as follows:



Never power down the MLB while the system is enrolling a module.

---

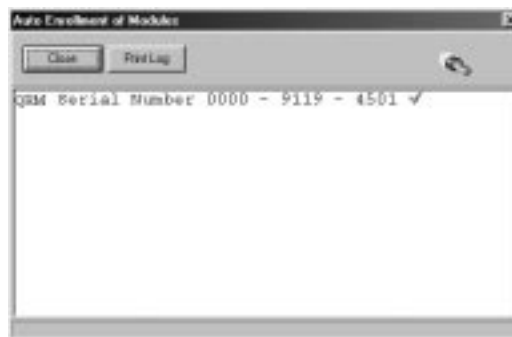


Start Scan

**(1) Click the *Start Scan* button.**

The system searches for the module. When the module is found, the system blinks the yellow service LED on the module, presents a screen message indicating that the module has been enrolled, and stops scanning for modules.

After the system has enrolled the module, a screen is presented that shows the module (with serial number) that has been enrolled.



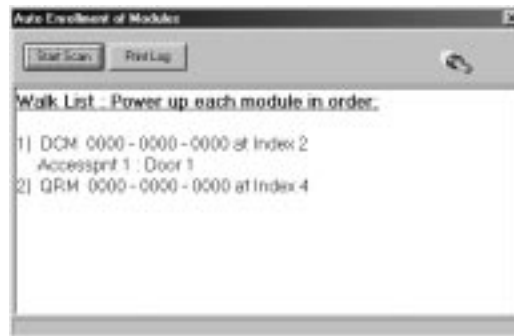
Close

**(2) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

**2b. Enrolling Multiple Modules.**

The Auto Enroll dialog box should already be on your screen, and should look something like this when enrolling multiple modules:



If the modules are powered up before the enrollment process or powered up in the wrong order, they will be enrolled incorrectly. Never power down the MLB during the enrollment process.




To enroll multiple modules into your PassPoint system, the modules must be powered up in the order that they are listed on the screen. To enroll the modules, proceed as follows:

- (1) **Click the *Print Log* button.** A “walk list” of all the modules waiting to be enrolled is printed.
- (2) **Verify the power is applied to the first module listed only.**

**NOTE:** You must power up the modules in the order in which they appear in the walk list. Be certain the subsequent modules are powered down when you begin the enrollment process. Once you start the scan and properly enroll each module, you may leave the module powered up.



A rectangular button with a black border and the text "Start Scan" in a sans-serif font.

**(3) Click the *Start Scan* button.**

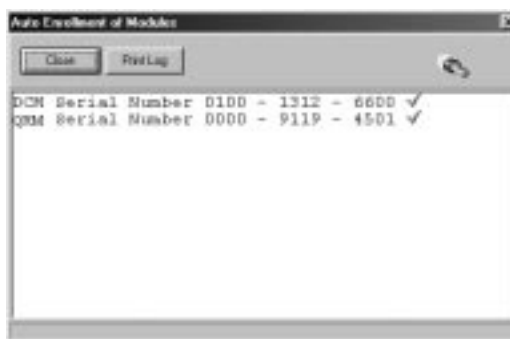
The system searches for the first module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. Next, a message will be displayed indicating that the system is polling for the next module in the “walk list.”

**(4) Apply power to the next module in the list.**

The system searches for the next module in the list. When the module is found, the system blinks the yellow service LED on the module, and presents a screen message indicating that the module has been enrolled. If additional modules are in the list, a message will be displayed indicating that the system is polling for the next module.”

**(5) Repeat the application of power to the modules, one at a time, until all modules have been enrolled.**

When the system has enrolled the last module in the list, the screen shows a listing of modules (with serial numbers) that have been enrolled.





**(6) Click the *Close* button.**

Enrollment has been successfully completed and the system will remove the Auto Enrollment of Modules screen.

**2. Click the *Start Scan* button.**

The system searches for the new module. When it finds it, a message appears indicating that the module has been enrolled.

The system then stops scanning for modules. If you were enrolling more than one module, you would have to wait until the system told you that all the modules had been enrolled.

## ***Configuring Modules***

When you configure a module, you're really telling the system how you want the module to operate and what functions you want it to perform. Each type of module can perform different tasks and contains different components. It's up to you to determine how these components are to operate in your system.

In addition to relays, which are used on DCMs and QRMs, there are other components to be configured, such as triggers (for DCMs and QRMs) and zones (for ZIMs).

Note that the below procedure described for module configuration may also be used to edit information on a module that was already configured.

To configure a module:

1. **In the Installer Configuration dialog box, right-click on the module you want to configure.**

A sub-menu of choices appears.

2. **Select *Properties* from the sub-menu.**

Selecting *Properties* calls up a dialog box for the module. This dialog box contains tabs and fields of information describing how the module functions. Each field can be modified to tailor the functioning of the module.

3. **Fill in the fields of the dialog box as applicable.**

The tabs and fields for each module type are different. Refer to the following sections for the applicable module type you are configuring for a description of each field.

4. **When you are finished, click *OK*.**

Once you click *OK*, you can download the database to save your changes. Refer to the section of this chapter titled “Download the Database” for information on performing this step.

## ***DCM setup dialog box***

The DCM Setup dialog box looks like the one below:



The dialog box contains nine tabs. Each tab contains fields that describe various functions and settings for control of the DCM. For a description of these fields, refer to Chapter 9 of this guide.

## ***QRM setup dialog box***

The QRM Setup dialog box looks like the one below:



The dialog box contains five tabs. Each tab contains fields that describe various functions and settings for control of the QRM. The tabs and their related fields are described below.

### ***QRM system tab***

**Serial Number** - You can enter the serial number for this module if you know it. If you have already auto-enrolled the module, the proper serial number should already appear here.

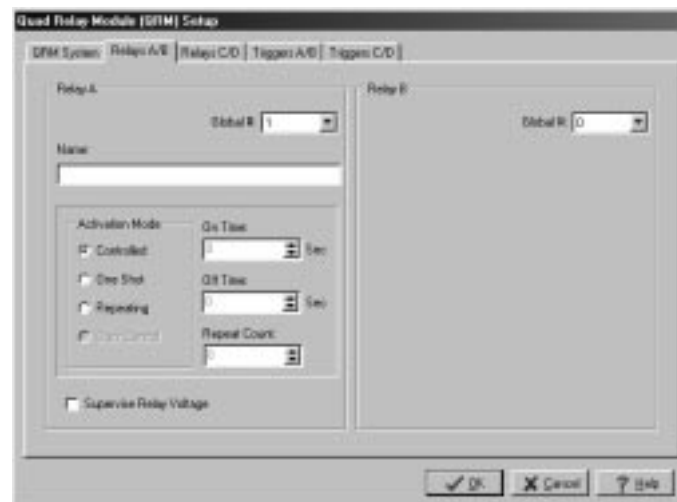
**Module Name** – If desired, you can enter a name for the module. The name entered will be displayed on the screen as a part of the QRM identification information.

**AC Power Supervision** - When this field is enabled, the module notifies the system when it experiences an AC loss condition. An event will be logged when the AC power is lost or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

**Low Battery Supervision** - When this field is enabled, the module will notify the system when it experiences a low battery condition. An event is logged when the low battery condition is detected and/or restored. This feature should be enabled on only one of the modules powered by the particular power supply.

### ***Relay tabs***

The dialog box has two Relay tabs: one for relays A/B, and one for relays C/D. The Relay tabs for A/B and C/D appear as shown below:



**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system automatically shows only the available numbers. Every relay must be given a unique global relay number.

**Name** - Use this textual field to enter a name for the relay you are defining.

**Activation Mode** - You can select from one of three modes:

- **Controlled:** The system or a user can command the relay On or Off.
- **One-Shot:** When commanded by the system or a user, the relay energizes for a specified number of seconds, then de-energizes. [1 - 65535 seconds]
- **Repeating:** When commanded by the system or a user, the relay energizes for a specified number of seconds, then de-energizes for a specified number of seconds. This cycle is repeated for a specified number of times or repeated indefinitely until commanded to stop. [On time = 1-65535 seconds] [Off time = 1-65535 seconds] [Repeat Count = 0 (Continuous) or 1-65535 counts]

**On Time** - This field is active only if you have chosen *One-Shot* or *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the relay should be activated.

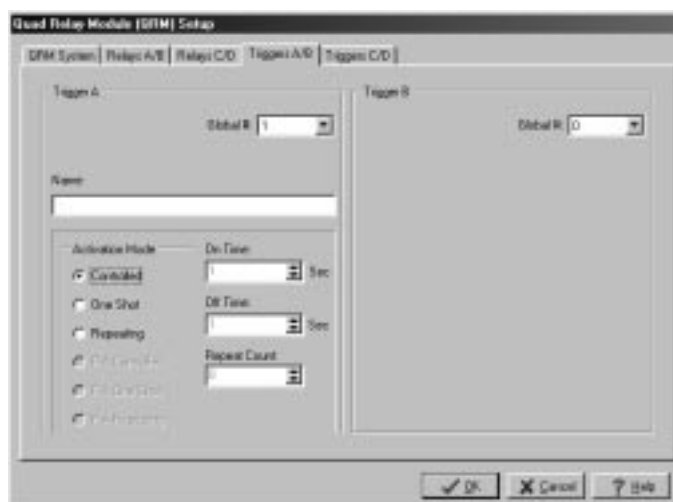
**Off Time** - This field is active only if you have chosen *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the relay should be deactivated before it activates again.

**Repeat Count** - This field is active only if you have chosen *Repeating* as the operating mode. Enter the number of times you want the relay to repeat its activate/deactivate cycle. You can choose any number from 0 to 65535. Note that a value of 0 causes the relay to repeat continuously until it is commanded off.

**Supervise Relay Voltage** - Select this field if you want to monitor the voltage going to the relay. If you select this field, the system continuously monitors the relay voltage and displays the status of the relay voltage on a separate status screen.

## Trigger tabs

The dialog box has two Trigger tabs: one for triggers A&B, and one for triggers C&D. The Trigger tabs for A/B and C/D appear as shown below:



**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system automatically shows only the available numbers. Every trigger used in the system must be given a unique global trigger number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the trigger you are defining.

**Activation Mode** - You can select from one of three modes:

- **Controlled:** The system or a user can command the trigger On or Off.



- **One-Shot:** When commanded by the system or a user, the trigger energizes for a specified number of seconds, then de-energizes. [1 - 65535 seconds]
- **Repeating:** When commanded by the system or a user, the trigger energizes for a specified number of seconds, then de-energizes for a specified number of seconds. This cycle is repeated for a specified number of times or repeated indefinitely until commanded to stop. [On time = 1-65535 seconds] [Off time = 1-65535 seconds] [Repeat Count = 0 (Continuous) or 1-65535 counts]

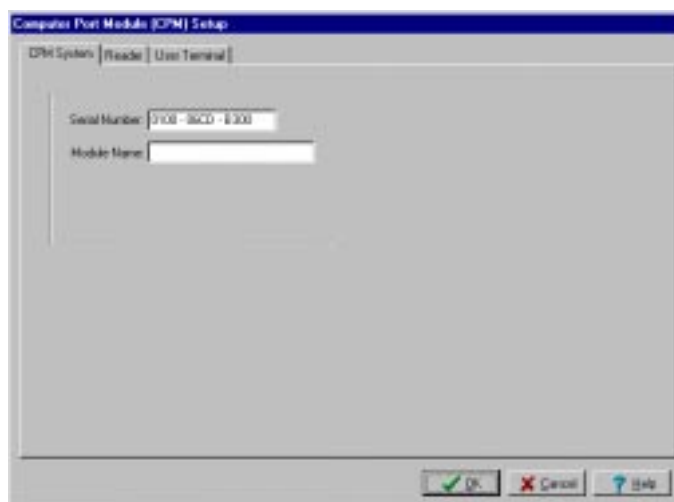
**On Time** - This field is active only if you have chosen *One-Shot* or *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the trigger should be actuated.

**Off Time** - This field is active only if you have chosen *Repeating* as the operating mode. Enter a time in seconds (1 - 65535) for how long the trigger should be deactivated before it activates again.

**Repeat Count** - This field is active only if you have chosen *Repeating* as the operating mode. Enter the number of times you want the trigger to repeat its activate/deactivate cycle. You can choose any number from 0 to 65535. Note that a value of 0 causes the trigger to repeat continuously until it is commanded off.

## ***CPM setup dialog box***

The CPM Setup dialog box looks like the one below:



The dialog box contains three tabs. Each tab contains fields that describe various functions and settings for control of the CPM. The tabs and their related fields are described below.

### ***CPM System tab***

**Serial Number** - You can enter the serial number for this module if you know it. If you have already auto-enrolled the module, the proper serial number should already appear here.

**Module Name** – If desired, you can enter a name for the module. The name entered will be displayed on the screen as a part of the CPM identification information.

### ***Reader tab***

**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system automatically shows only the available numbers. Every reader used in the system must

be given a unique global reader number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the reader you are defining.

**Type** - This field selects the reader technology type. Use the drop-down list to select the desired type. The allowable selections are:

- **Wiegand Card**
- **Prox Card**
- **Mag Stripe Card**
- **Keypad Only**
- **Wiegand/Keypad Combination Unit**
- **Prox/Keypad Combination Unit**
- **Mag Stripe/Keypad Combination Unit**

Note that Keypad Only and the Combination Units **MUST NOT** be used by a reader that is performing an enrollment function.

**Function** - This field selects the function for the uncommitted reader. Setting this field to Enrollment Reader at User Terminal x selects this reader to send card numbers to the indicated User Terminal when the user is in any field where a card number must be entered. This allows the reader to be used as an Enrollment Station. Setting this field to Command Reader selects this reader to allow card swipes that can initiate actions within the system. The actions can be programmed through the event/action setting of the system or through the actions assigned to individual cardholders.

**Interface** - The electrical specifications for the reader connected to this interface must be specified in this field. Most units adhere to

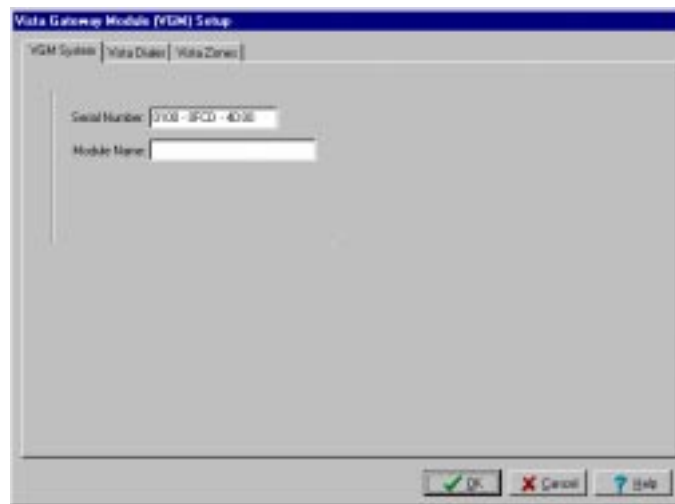
the Data1/Data0, or Wiegand, wiring standard, even if the card reader is not a Wiegand card reader. Many magnetic stripe card readers conform to the Clock/Data interface method. You must specify the corresponding electrical interface type used by the readers you are installing by selecting the appropriate interface type.

### ***User Terminal tab***

Selections under this tab are not currently used and are reserved for future product enhancements.

## ***VGM setup dialog box***

The VGM Setup dialog box looks like the one below:



The dialog box contains three tabs. Each tab contains fields that describe various functions and settings for control of the VGM. For a description of these fields, refer to Chapter 11 of this guide.

## **ZIM setup dialog box**

The ZIM Setup dialog box looks like the one below:



The dialog box contains five tabs. Each of these tabs contains fields that describe various functions and settings for control of the ZIM. Each of the tabs and their related fields are described below.

### **ZIM System tab**

**Serial Number** - You can enter the serial number for this module if you know it. If you have already auto-enrolled the module, the proper serial number should already appear here.

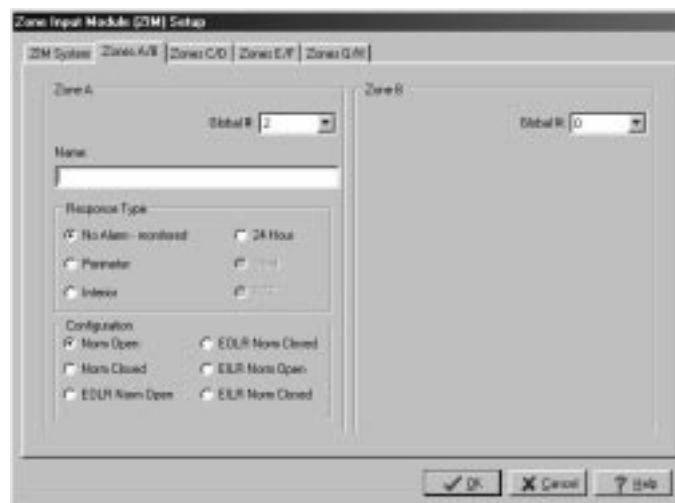
**Module Name** – If desired, you can enter a name for the module. The name entered will be displayed on the screen as a part of the ZIM identification information.

**AC Power Supervision** - When this field is enabled, the module will notify the system when it experiences an AC loss condition.

An event will be logged when the AC power is lost or restored. This feature should only be enabled on one of the modules powered by the particular power supply.

### **ZIM Zone tabs**

The dialog box has four Zone tabs. Each tab contains information about two different zones. The Zone tabs for A/B, C/D, E/F, and G/H appear as shown below:



The uncommitted zone inputs provided by the PassPoint system are for supplemental functions such as signaling certain conditions. They have not been tested for UL compliance and as such cannot be used for burglary functions in UL installations.

**Global #** - This field selects the number of this resource from the total number of resources available. Use the drop-down list to select from the available values. The system automatically shows only the available numbers. Every zone used in the system must

be given a unique global zone number if it is not being used for an access point.

**Name** - Use this textual field to enter a name for the zone you are defining.

**Response Type** - Select a response type for the zone. You can select from four different options:

- **No Alarm-Monitored:** This allows the zone to be seen by the system and to trap faults/restores. No alarm zones are used primarily by event/action relations and system scripts.
- **Perimeter:** Faults/Restores are always recognized on this zone, but can only generate an alarm when the burglary system is armed AWAY or STAY. A perimeter zone will restore when the zone returns to normal (zone will latch if system is armed).
- **Interior:** Faults/Restores are always recognized on this zone, but can only generate an alarm when the burglary system is armed AWAY. All Interior zones are temporarily ignored for the first 2 minutes after arming AWAY. An Interior zone will restore once the zone returns to normal (zone will latch if system is armed).
- **24-Hour:** Faults/Restores are always recognized on this zone. An alarm is generated whenever this zone is faulted. A 24-Hour zone will restore once the zone returns to normal.

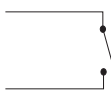
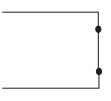
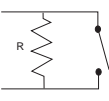
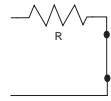
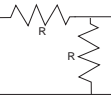
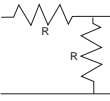
**Configuration** - Select a configuration for the zone. You can select from one of the following:

- Normally Open
- Normally Closed

- EOLR Normally Open

**NOTE:** EOLR and EILR zones require ADEMCO's standard 2K-Ohm end-of-line or end-in-line resistors.

- EOLR Normally Closed
- EILR Normally Open
- EILR Normally Closed

Normal Sensor State	ZONE STATES					
	TWO-STATE ZONE (unsupervised)		THREE-STATE ZONE (EOLR supervised)		FOUR-STATE ZONE (EILR supervised)	
	Normally Open (N.O.)	Normally Closed (N.C.)	Normally Open (N.O.)	Normally Closed (N.C.)	Normally Open (N.O.)	Normally Closed (N.C.)
0 (short)	FAULT	NORMAL	FAULT	TROUBLE	TROUBLE (SHORTED)	TROUBLE (SHORTED)
R	NA	NA	NORMAL	NORMAL	FAULT	NORMAL
2R	NA	NA	NA	NA	NORMAL	FAULT
infinite (open)	NORMAL	FAULT	TROUBLE	FAULT	TROUBLE (OPEN)	TROUBLE (OPEN)
Sensor Connections						
MLB ZONES	√	√	√	√		
DCM ZONES	√	√	√	√		
ZIM ZONES	√	√	√	√	√	√

## Download the Database

The last step in getting your module enrolled is to download the database.

1. Close the Installer Configuration dialog box.



At close, the system will automatically ask you if you want to download the database.



**2. Click Yes.**

The Download dialog box appears. At the top of the dialog box is the account number you will be downloading. Make certain that you are downloading to the correct account. There are also checkboxes in the dialog box that tell you what information you will be downloading. These checkboxes are automatically checked for you according to the system options you have changed.



If there are specific options you want to download that have not been selected automatically, you can select them now by clicking in the applicable checkboxes.

**3. Click Start.**



---

The database download now proceeds.

## Appendix

# A

## *Wiring Considerations*

When installing your PassPoint system, there are several wiring factors that need to be considered. This appendix explains the various wiring topologies and provides details about wiring specifications.

## ***Wiring Considerations***

Before selecting sites for your various system cabinets, you should understand how the system is wired together.

All system modules communicate with the Main Logic Board via a twisted-pair network technology. This connection supports communications with up to 126 peripheral modules. Each module connected to the network is considered a “node.” If you are using a PassPoint Access Starter Kit, you have two nodes: an MLB and a DCM, both of which have their own serial numbers. You can, however, expand your system by adding additional nodes. For example, you can add another DCM to control two more access points.

When you are wiring the system and selecting installation sites for your components, there are several factors you must keep in mind. These factors are described on the following pages.



The wiring method and installation locations recommended in this manual are in accordance with the National Electrical Code ANSI/NFPA 70.

---

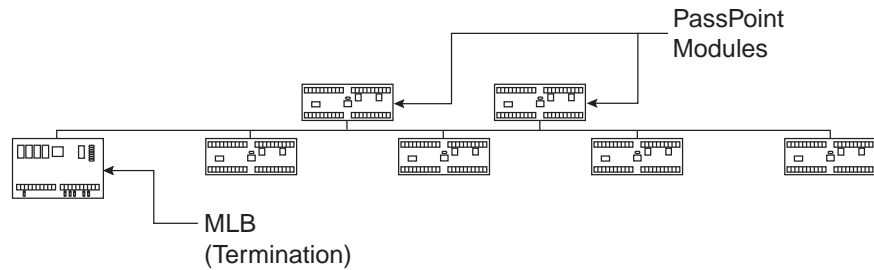
## ***Topology***

The system’s unshielded twisted-pair wiring technology is designed to support free-topology wiring, and accommodates bus, star, loop, or any combination of these topologies. PassPoint modules can be located at any point along the network wiring. This capability simplifies system installation and makes it easy to

add modules if the system ever needs to be expanded. The five different wiring topologies are represented in the following diagrams.

*This wiring topology is terminated at the MLB using a 52.3-ohm resistor across the network terminals (15 & 16) of the MLB.*

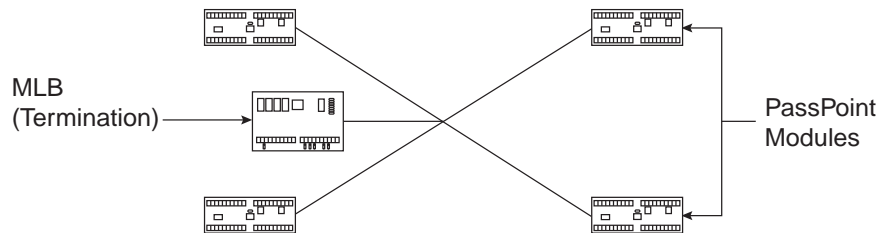
*NOTE: Total wire length  $\leq$  1,500 ft*



### Singly Terminated Bus Topology

*This wiring topology is terminated at the MLB using a 52.3-ohm resistor across the network terminals (15 & 16) of the MLB.*

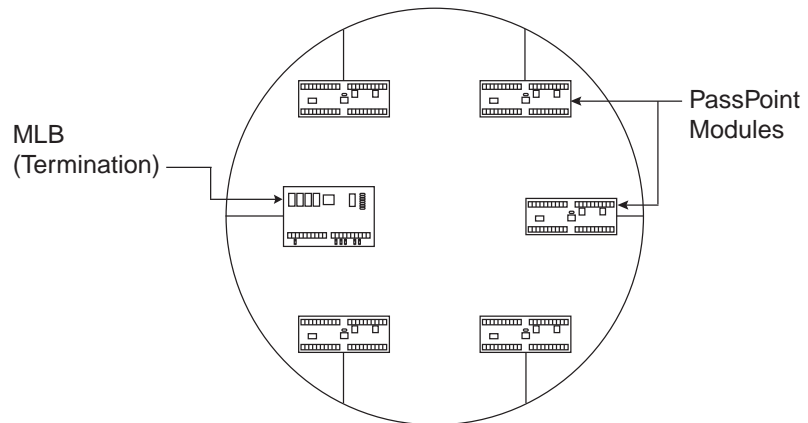
*NOTE: Total wire length  $\leq$  1,500 ft*



### Star Topology

*This wiring topology is terminated at the MLB using a 52.3-ohm resistor across the network terminals (15 & 16) of the MLB.*

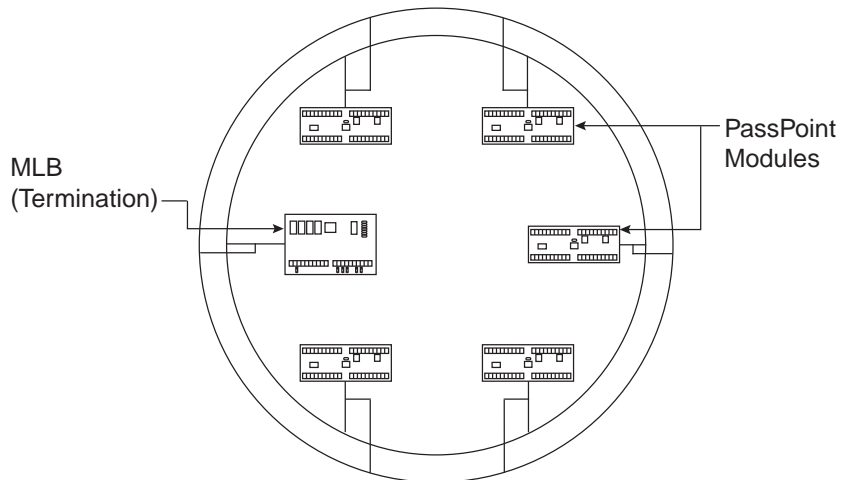
*NOTE: Total wire length  $\leq 1,500$  ft*



**Loop Topology**

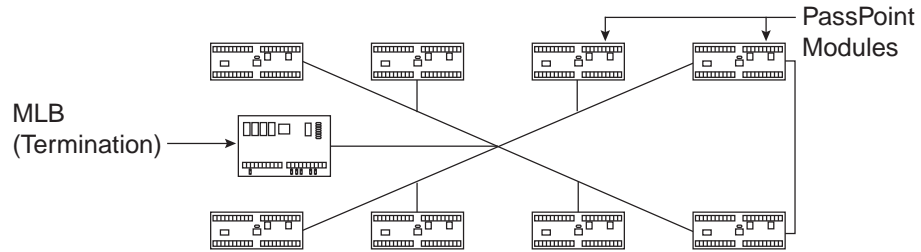
*This wiring topology is terminated at the MLB using a 52.3-ohm resistor across the network terminals (15 & 16) of the MLB.*

*NOTE: Total wire length  $\leq 1,500$  ft*



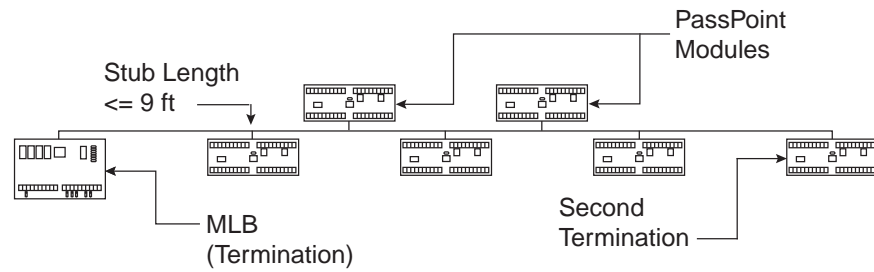
**Redundant Loop Topology**

This wiring topology is terminated at the MLB using a 52.3-ohm resistor across the network terminals (15 & 16) of the MLB.  
NOTE: Total wire length  $\leq 1,500$  ft



### Combination Loop/Bus Topology

This wiring topology is terminated using a 105-ohm resistor across the network terminals of the two farthest modules. The MLB does not have to be one of the termination sites.  
NOTE: Total wire length  $\leq 1,500$  ft



### Doubly Terminated Bus Topology

Free-topology specifications:

(Can be singly terminated bus, star, loop, or loop/bus combination)

Table 1:		
Cable Type	Max. node-to-node distance	Max. total wire length
Belden 85102	1500 feet	1500 feet
Belden 8471	1500 feet	1500 feet
Level IV, 22 AWG	1500 feet	1500 feet

**Doubly terminated bus specifications:**

<b>Cable Type</b>	<b>Max. bus length</b>
Belden 85102	8000 feet
Belden 8471	8000 feet
Level IV, 22 AWG	4000 feet

---



When planning your wiring scheme, keep in mind that using shielded wiring will drastically reduce the allowable wire run lengths.

---

**RS-232 cabling:**

Standard, 9-conductor, shielded, 22 AWG cable, 50 feet (null modem)

---



Refer to the cable drawings in Chapter 3 if a longer RS-232 Cable is required.

---

**Keypad wiring:**

22 AWG, 3 feet

(The keypad should be mounted on the cabinet only and not wired through the premises.)

**Power Harness:**

Use power harness SA12160 only (supplied). (Local and remote power outputs of power supply.)



**Door strike power:**

Depends on wire gauge and current requirements of the door strike or magnetic lock. Probably about 500 feet of 16 AWG wire for 350mA of current.

**Reader interfaces:**

200 feet of 22-gauge  
300 feet of 20-gauge  
500 feet of 18-gauge

**Color code of termination resistors:**

52.3 ohm - Green, Red, Orange, Gold, Brown  
105 ohm - Brown, Black, Green, Black, Brown

## ***Wiring notes***

Keep reader, Echelon, and RS-232 wiring away from any high-current wiring. This includes the door strikes, as well as any building wiring that delivers power to “noisy” load (AC units, refrigerators, etc.).



---

We suggest using an electric suppressor such as EL-EDS (manufactured by EDCO) to provide transients protection for magnetic locks/door strikes and relay contacts. Install one suppressor as close as possible across the leads connected to the lock. Install a second suppressor across the relay terminals at the other end of the lock cable.

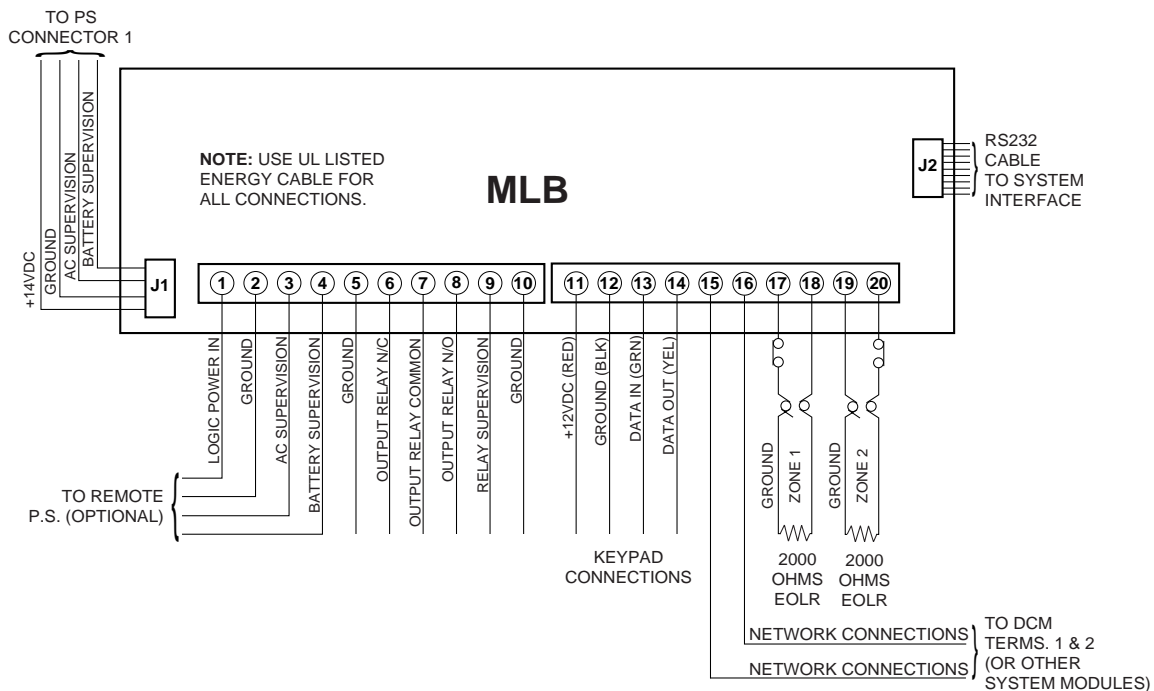
---

## **Wire characteristics**

<b>Cable Type</b>	<b>Wire Dia./AWG</b>	<b>Rloop Ohm/km</b>	<b>C nF/km</b>	<b>Vprop % of c</b>
Belden 85102 Single twisted-pair, stranded 9/29, unshielded, plenum	1.3mm/16A WG	28	56	62
Belden 8471 Single twisted-pair, stranded 9/29, unshielded, non- plenum	1.3mm/16A WG	28	72	55
Level IV 22AWG Single twisted-pair, typically solid & unshielded	0.65mm/22A WG	106	98	41
JY (St) Y 2x2x0.8 4 wire helical twist, solid, shielded	0.8mm/20.4 AWG	73	98	41

## Main Logic Board Connections

Wire the MLB according to the diagram below:



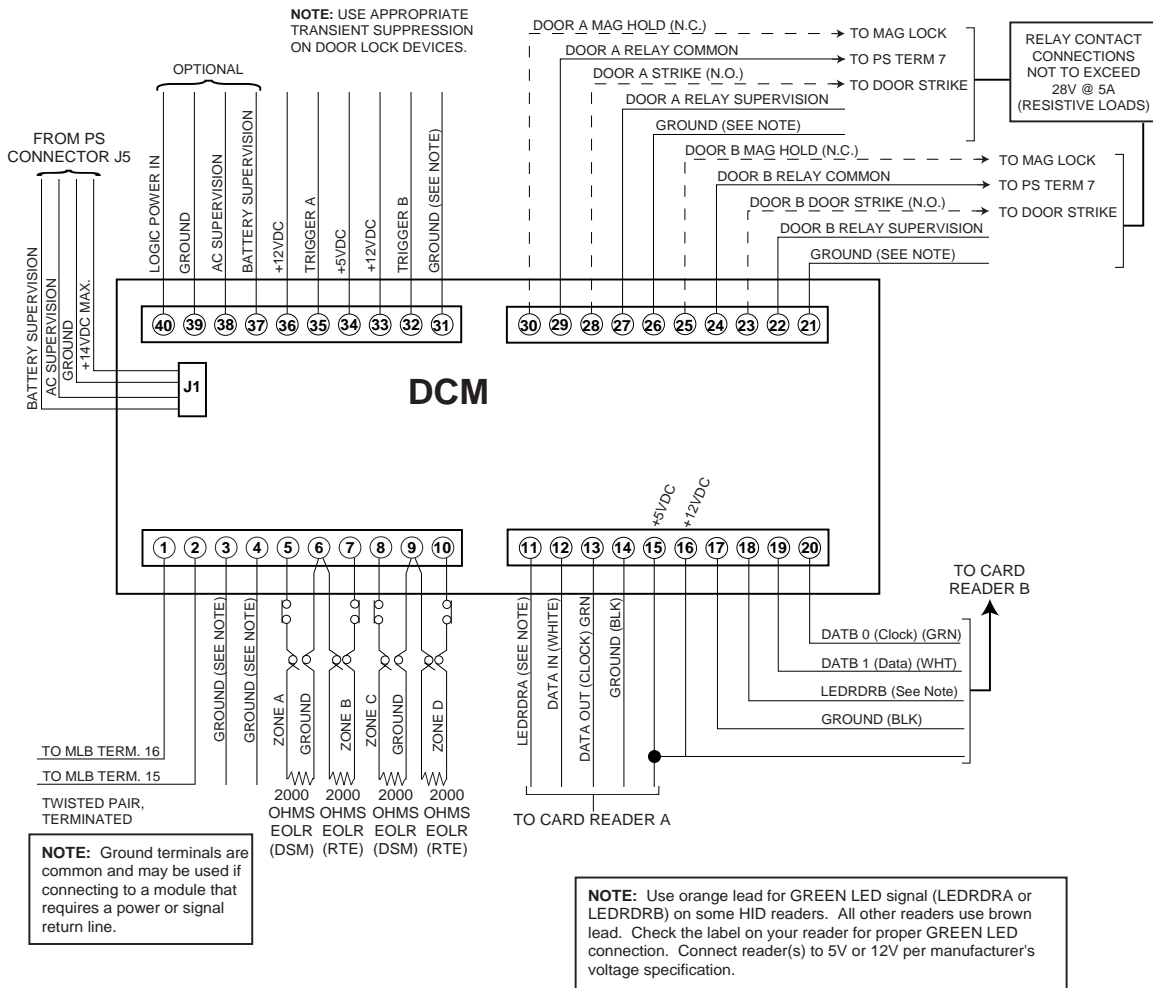
MLB Battery Support ADEMCO Part Number N7673. 3V Lithium Battery estimated standby lifetime: 10 years.

**CAUTION** - Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries in accordance with the manufacturer's instructions. Battery type: Lithium battery type 2025.

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

# Door Control Module Connections

Wire the DCM according to the diagram below:



## Power Supply Specifications

Transformer part number N8167:	120VAC PRIM. (60 Hz) 18VAC 50VA SEC.
<b>Note:</b> Connect transformer to 24-hr. wall outlet.	
Switching Regulator Output:	13.3V +/- 1.2VDC @ VAC Input: 102V-132V Vripple 600mVpp
Linear Regulator for Local Power Output:	13.7VDC @ 450mA
Total Power Supply Output Current:	1.8A +/- 200mA
Door Strike/Mag Lock Max. Current:	900mA
J1 Local Logic Power Output:	450mA max.
J5 Logic Power Output:	450mA max.
Battery Backup:	12V/7AH



---

Connection to terminal blocks 9 and 10 is not required for AC and battery supervision when power harness SA12160 is used with J1 and J5. If SA12160 power harnesses are not used, connect Low Battery and AC Loss supervision terminals from power supply to Low Battery and AC Loss supervision terminals of system modules. AC Loss and Low Battery supervision outputs are provided for supervision of up to two PassPoint modules.

---



## Appendix

# B

## *Firmware Download*

When a system has been installed for a long period of time, you may be instructed to download new firmware into the MLB for compatibility with later PassPoint software. This appendix provides the procedures for downloading the PassPoint MLB firmware.

**NOTE:** Never replace the firmware in the MLB unless instructed to do so.

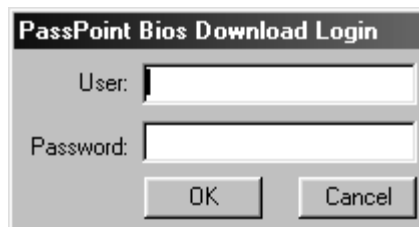
## ***Downloading MLB Firmware***

When a firmware download is required for an installation, the new MLB data will be provided to you as a file with a .MLB extension. In cases where the firmware is part of a PassPoint program upgrade, the firmware is contained in a PassPoint sub-directory named Updates.

To download new MLB firmware, follow the procedure below:

- 1. Close *PassPoint Plus* if it is running on your computer.**
- 2. Click on your Windows *Start* button.**
- 3. In Programs, go to *PassPoint Plus* and select *MLB Firmware Downloader*.**

The MLB Firmware Downloader loads and the following screen is displayed:



- 4. Enter your User Name and Password.**

The user name and password are the same as what you have defined as the Installer's user name and password in *PassPoint Plus*.

- 5. Click *OK*.**

The following MLB Firmware Downloader screen is displayed:





**6. Click *Start*.**

The following MLB Firmware Downloader screen is displayed:



**7. Click *Next*.**

The following Account Navigator screen is displayed:



8. Select the account for the MLB that is to receive a firmware download using method a. or b. below:
  - a. If you have just one MLB defined in your computer, its account is automatically selected.
  - b. If you have several MLB's (accounts) controlled by the computer, you may locate the account as follows:
    - (1) Click on the down arrow to the right of the *Search By* field. A drop-down list appears where you can elect to search by account name or number.
    - (2) Select the method of search you prefer.
    - (3) In the *Search For* field, start typing your desired account name or number. As you enter data, the system will display the closest match it finds in your database. When the correct account is displayed in the *Search For* window, discontinue typing the data.
9. Click **OK**.

The selected account is opened, the computer connects to the MLB, and the following MLB Firmware Downloader screen is displayed:



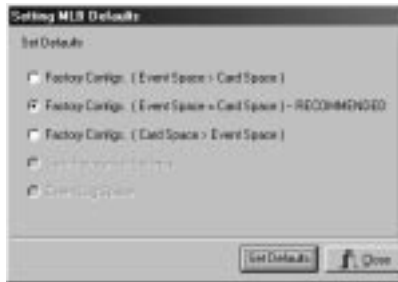
**10. Click *Next*.**

The following MLB Firmware Downloader screen is displayed:



**11. Click *Next*.**

The following Setting MLB Defaults screen is displayed:



**12. Click on the desired *Factory Configs*.**

**NOTE:** We recommend that you use the Factory Configuration already selected.

**13. Click *Set Defaults*.**

The MLB resets to the selected default settings. After the MLB resets (approximately 2 minutes), the following MLB Firmware Downloader screen is displayed:



**14. Click *Next*.**

The following MLB Firmware Downloader screen is displayed:



- 15. The screen automatically has *MLB File* selected. Leave this selection as it is and click *Next*.**

The following Open screen is displayed:



The directory is automatically set to Updates. If this directory is not where your MLB firmware update is located, change the directory as necessary.

- 16. Click on the file name for your MLB firmware update and then click *Open*.**

The following MLB Firmware Downloader screen is displayed:



**17. Click *Next*.**

The download of the MLB firmware starts and the following MLB Firmware Downloader screen is displayed:



The MLB firmware download takes a few minutes. When the download is complete, the MLB Firmware Downloader screen looks similar to the screen shown below:



**18. Click *Next*.**

The following MLB Firmware Downloader screen is displayed:



**19. Click *Finished*.**

The firmware in the MLB has been updated.

The MLB was defaulted to factory settings during the firmware upgrade. For proper operation, all account information must now be reloaded into the MLB using the procedures in the following paragraph.

## Downloading Account Information

Following the update of MLB firmware, the MLB must be defaulted and the account and cardholder databases must be reloaded into the MLB.

To default the MLB and download the required databases, follow the procedure below:

1. **Load PassPoint *Plus* and connect to the account where the MLB firmware was updated.**
2. **From the PassPoint *Plus Control* menu shown below, select *Set Defaults*.**



The Enter Password screen is displayed.



3. **Enter your Installer Password and click *OK*.**

The following Setting MLB Defaults screen is displayed:





4. Click on the *Full Default* desired. We recommend that you use the *Full Default* that is already selected. Next, click *Set Defaults*.

The Confirm screen shown below is displayed:



5. Click *Yes*.

The default values are loaded into the MLB.

6. From the *Config* menu shown below, select *Download*.



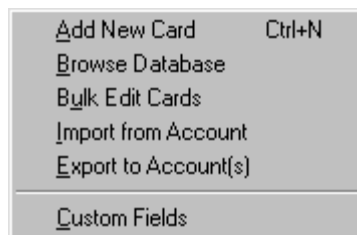
The following screen is displayed:



7. Click a check mark in the *All* box and click *Start*. The computer will download the MLB.
8. From the *Config* menu shown below, select *Cards*.



The following screen is displayed:



9. Select **Browse Database**. When the Card Data screen shown below appears, click on the **Summary** tab.



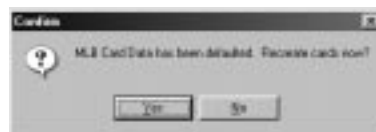
10. Click **Clear MLB**.

The Confirm screen is displayed.



11. Click **Yes**.

The cardholder database is cleared from the MLB and the following screen is displayed:



12. Click **Yes**. The card database in the MLB is recreated.



---

All required databases have been downloaded to the MLB and the system is ready for use.

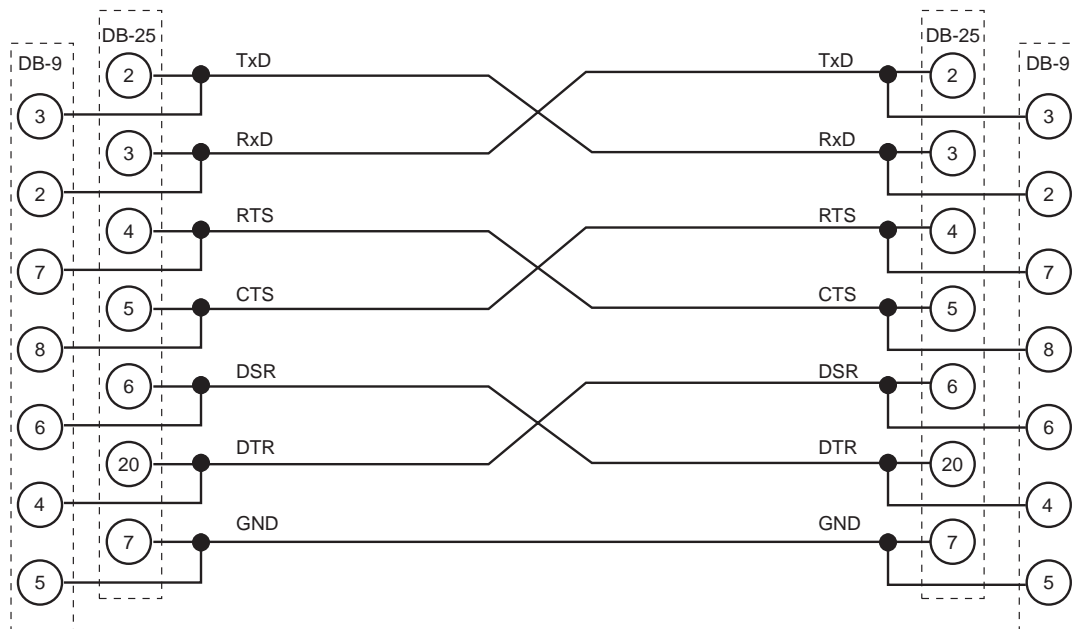
## Appendix

# C

## *Wiring Reference*

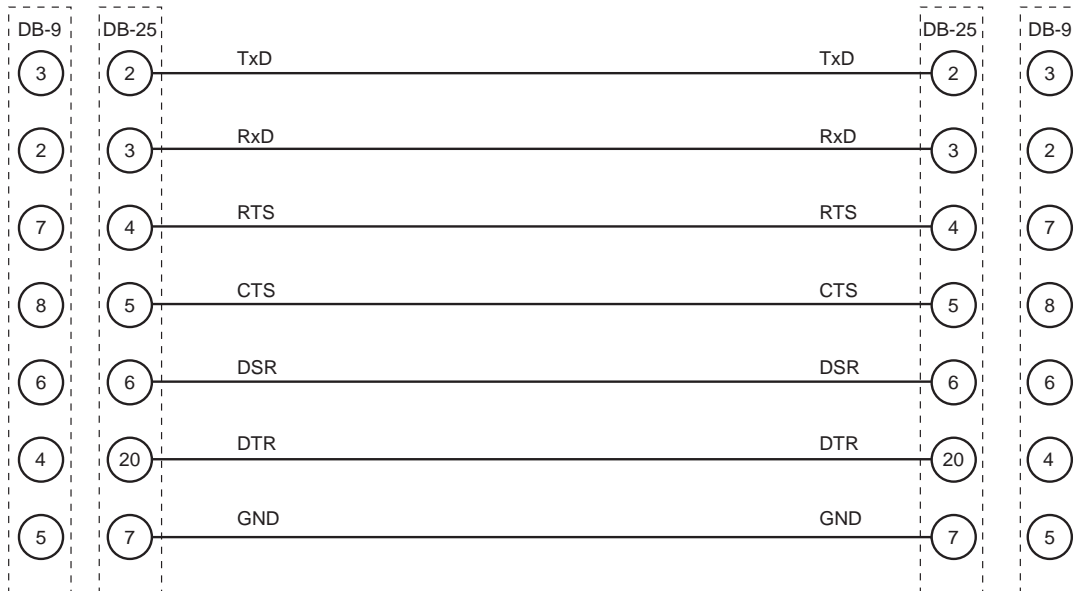
Cable diagrams and module connection diagrams, with installation procedures, are provided throughout this document. For quick reference, this appendix repeats all of the diagrams.

## Null Modem Cable



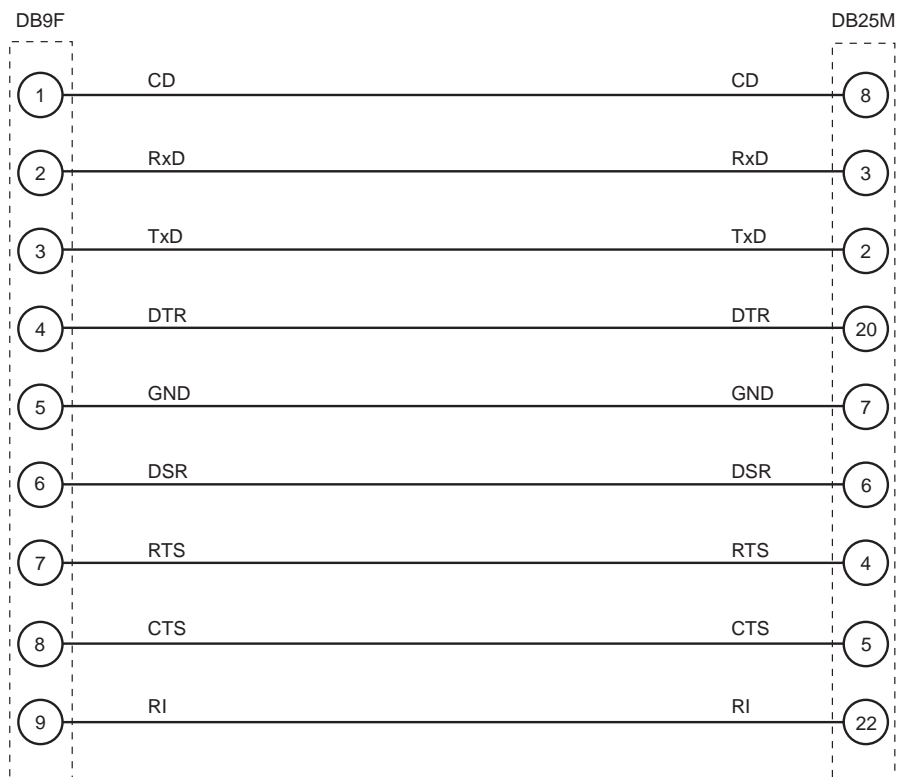
NOTE: UNUSED PINS NOT SHOWN

## Extension Cable



NOTE: UNUSED PINS NOT SHOWN

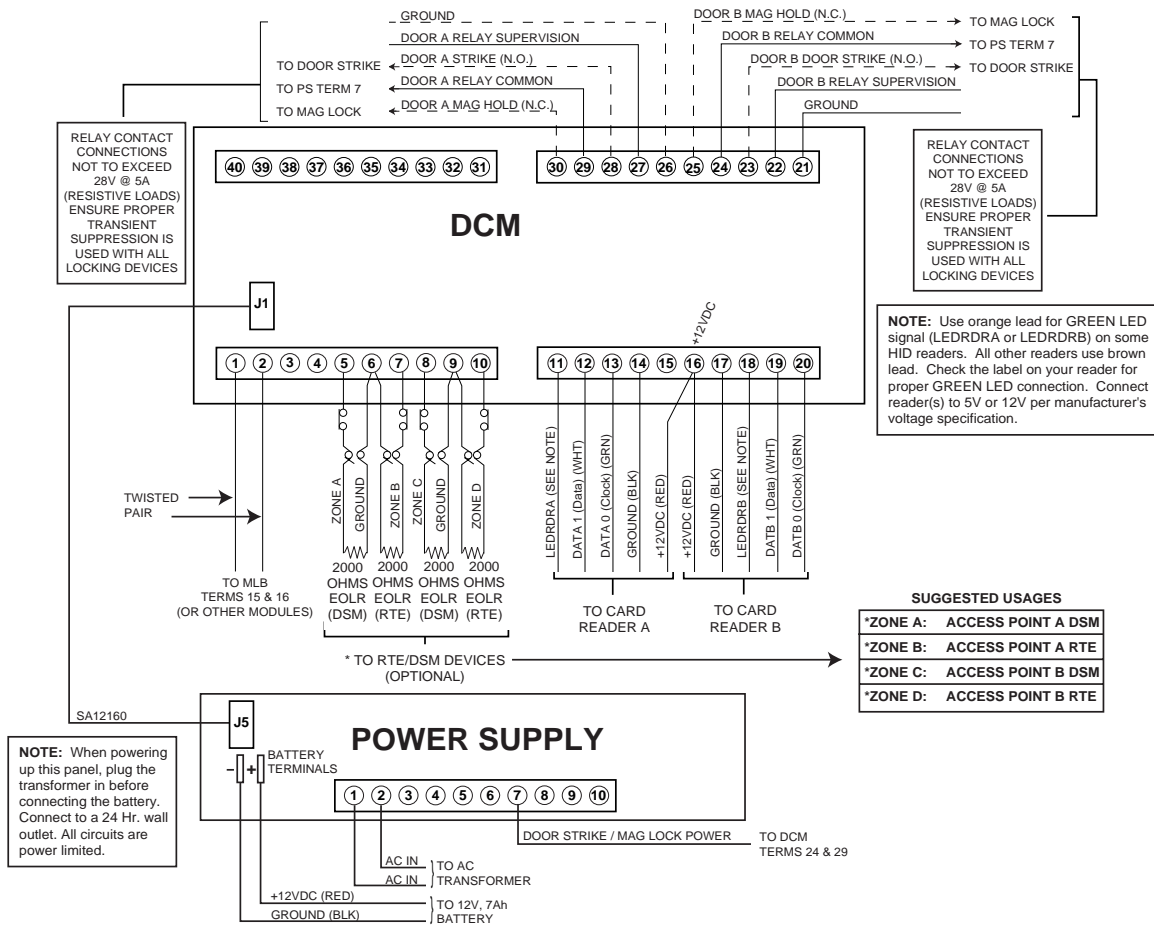
## Modem Cable



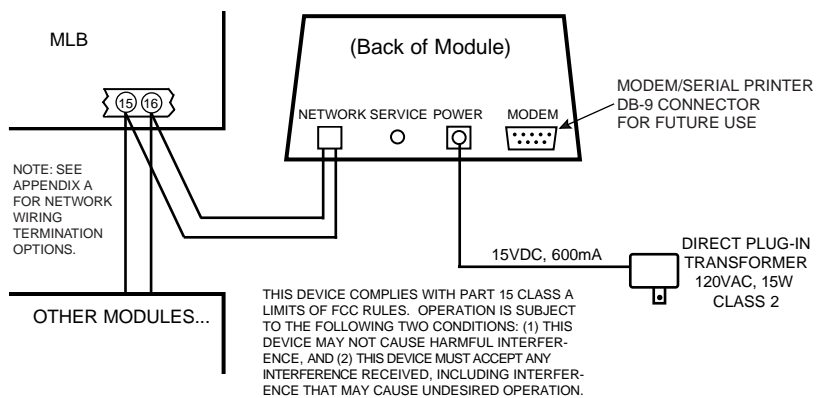
NOTE: UNUSED PINS NOT SHOWN



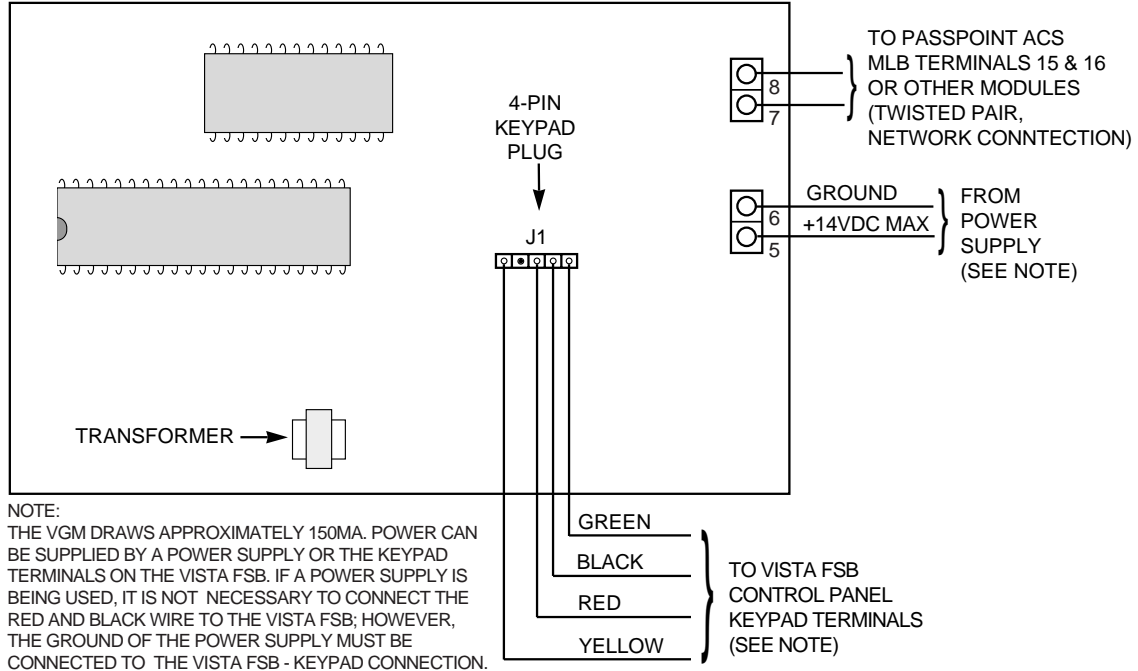
# Door Expansion Kit



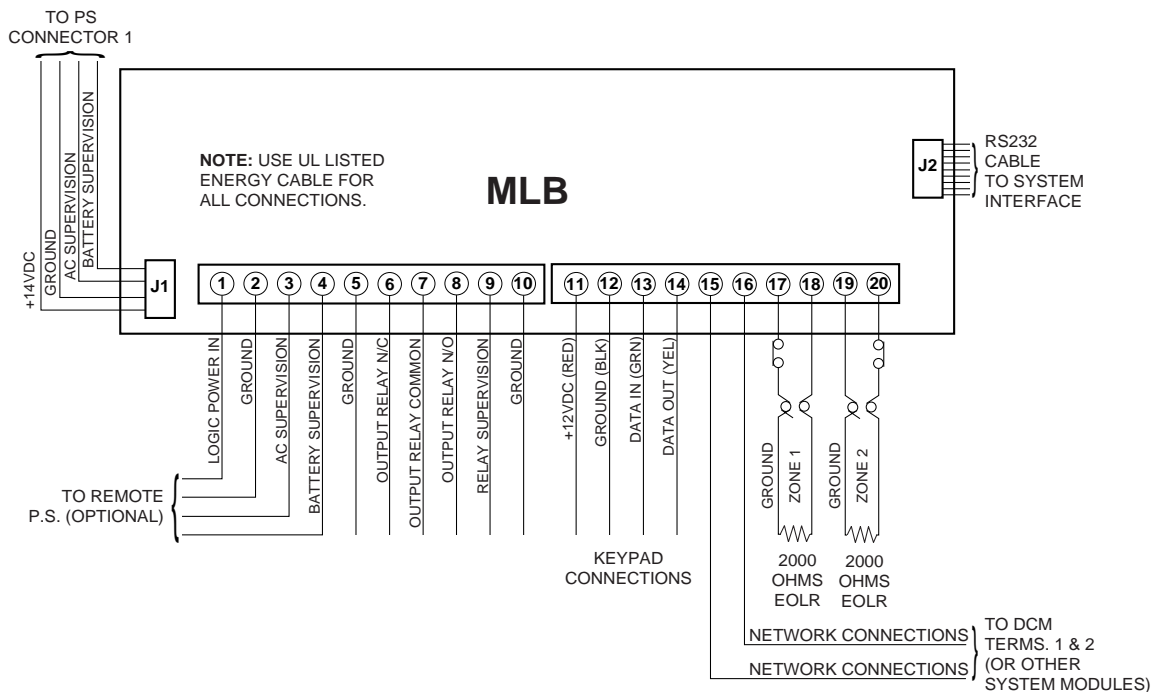
## Card Enrollment Kit



## VISTA Gateway Module



# Main Logic Board

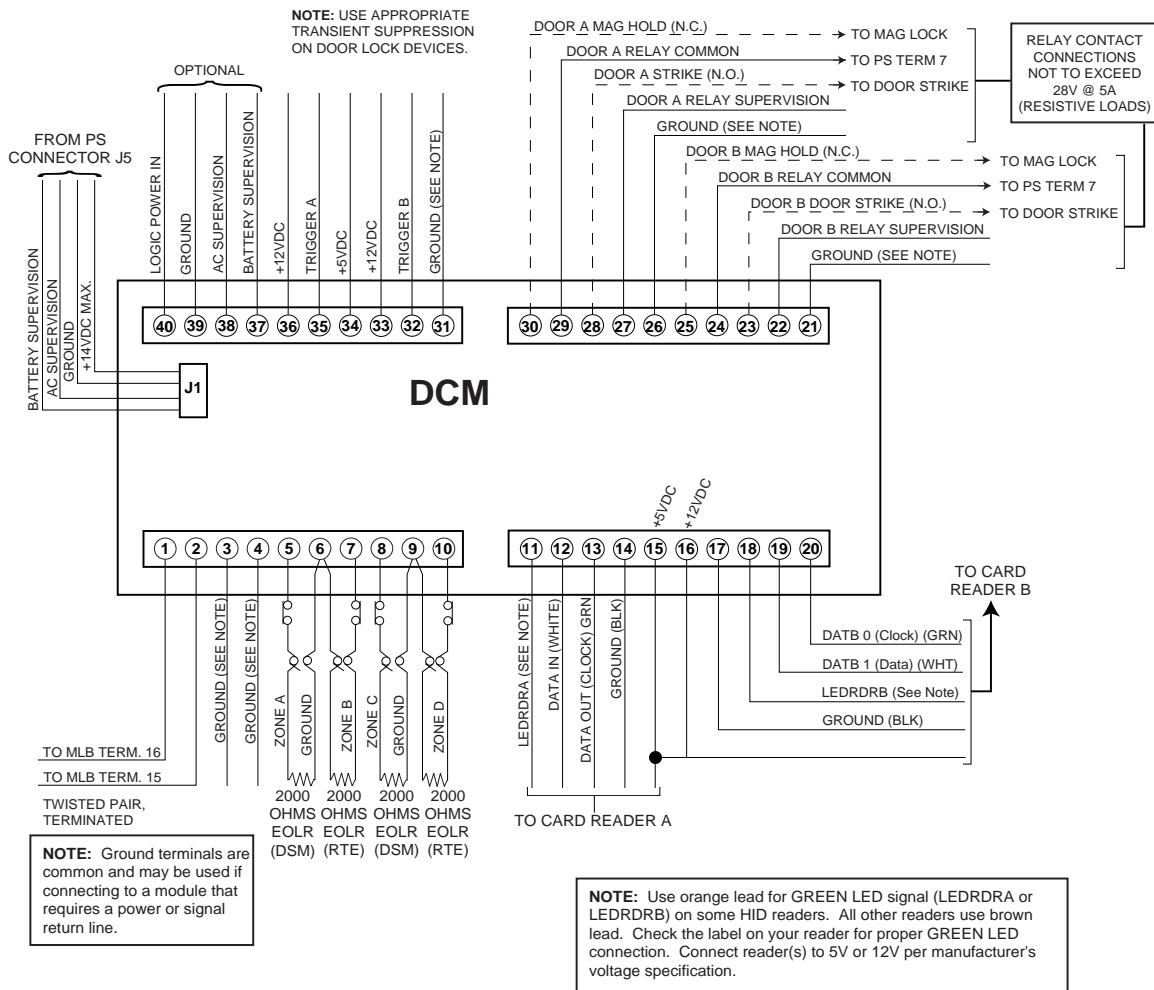


MLB Battery Support ADEMCO Part Number N7673. 3V Lithium Battery estimated standby lifetime: 10 years.

CAUTION - Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries in accordance with the manufacturer's instructions. Battery type: Lithium battery type 2025.

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

# Door Control Module





## Appendix

# 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 who share common access privileges regarding associated access points (doors) and times. The access group defines the access privileges of the individuals. All members of an access group have identical access privileges.

**Access Level** - The type of access permissions assigned to a cardholder.

**Access Partition/Access Area** - A completely enclosed space that is controlled for entry and egress. Generally, PassPoint notes when a person passes into the 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 is not notified when a person leaves the area. This leads 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 that define his/her access capabilities. Access privileges consist of the specifications of when and where a person may gain access or be allowed egress from a controlled area.

**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. A good example of such a situation is a boss who tries to pass his card back to his secretary in a parking garage, so that they may both park in the executive 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 card is presented to an entry reader after access has been granted on that card at the same reader, an anti-passback violation occurs. Based on the configuration of the access control system, the cardholder may be denied access as a result of that violation. In ADEMCO’s implementation, an anti-passback violation occurs when there is an attempt to use the same access point in the same direction a second time within a specified period of time without first using that access point in the opposite direction).



**Archive** - A file stored on your system's computer 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 to 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 zone types.

## ***B***

**Biometrics** – A reader technology that identifies 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 system may examine his access

privileges and determine if he 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 enters an assigned Personal Identification Number (PIN code). In situations where higher security is required, the entry reader may be a combination keypad/card reader unit.

**Cardholder** - An occupant of a premises who has been issued an access card or access code (or PIN, Personal Identification Number) that 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 serves 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 with a single card reader, or with a card reader/keypad combination unit 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** - An electromechanical switch that is used to control the flow of electricity to the door locking mechanism. The door control relay provides a “form C” dry contact set for an

output. In this way it can be used to introduce or eliminate current flow to an external device.

**Door Open Time** - The amount of time 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 that releases a locking mechanism.

**DSM (Door Status Monitor)** - A zone in an access control system committed to the monitoring of a door sense switch. The door sense switch reflects the state of the door (open or closed) and also allows the PassPoint to determine if the door has been forced open, or held open too long.

**Duress** - A condition in which a cardholder is 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*

**EILR Supervision (End In Line Resistor Supervision)** - A mode that is used to detect when someone has cut or shorted a cable monitoring a zone, such as a door sense switch. A resistor can be placed in the zone's circuit at the protected point, such that the controller can detect line trouble, in addition to fault and normal conditions.

**Enrollment Reader** - A card reader (connected to a CPM) that 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 the system may examine their access privileges to determine if they should be allowed to pass into the protected area. The term is “entry reader” because in most cases, the device is a card reader at which a cardholder must present his ID card. However, the device may be a keypad at which the individual must enter his assigned Personal Identification Number (PIN code). In some cases, where higher security is required, the entry reader may be a combination keypad/card reader unit.

**EOLR Supervision (End-of-Line Resistor Supervision)** - A mode that is used to detect when someone has cut or shorted a cable monitoring a zone, such as a door sense switch. A resistor can be placed in the zone’s circuit at the protected point, such that the controller can detect line trouble, in addition to fault and normal conditions.

**Event/Action 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 that 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 accepts only exit requests. Entry requests are ignored.

**Exit Reader** - An input device that is installed on the exit side of an access point door. At this device, individuals are required to identify themselves to the system so that the system may examine their access privileges 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) that 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 that automatically unlocks in the event of power loss.

**Fail Secure** - A locking device that automatically locks in the event of power loss.

**Force Arm Away** – A feature that arms the burglary system in the Away mode. Any faulted zones are automatically bypassed.

**Force Arm Stay** – A feature that arms the burglary system in the Stay mode. Any faulted zones are automatically bypassed.

**Forgive (Entry/Exit, Anti-Passback)** – A function that permits the administrator to “forgive” anti-passback and entry/exit violations so that the cardholder will not be “stuck” in the place where the violation is detected if their card swipes are denied. When this function is 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 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** – A feature that denies access to a cardholder in violation of anti-passback rules.

**Hard Entry/Exit** - A feature that denies access to a cardholder in violation of entry/exit rules.

**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 generally resembles a telephone keypad with respect to the relative positions and key name assignments.

- L**                      **Locked (Access Point)** - A mode that latches the door of the access point, disabling its readers for access control functions. The access point does 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 by the strong magnetic field. The door can be released (or “unlocked”) by interrupting the flow of current through the coil, thereby removing the strong magnetic field.
- MLB (Main Logic Board)** - 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 is also 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 on a keypad, allows 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)** - A sensor detection technology that senses movement within a specific area and changes 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 provider of 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 test results are provided to the modules, and ultimately to the MLB.

**Pre-Alarm Trigger Time (P-A Time)** - The amount of time, in seconds, before the start of an access point Door Open alarm, at which time the pre-alarm device is energized.

For example, if the door is set to 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 then gives 10 seconds of warning to whoever is holding the door open. If the door is still open at the end of the 30 seconds, a Door Open Timeout Alarm Event occurs. The pre-alarm device remains 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 that identifies 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)** – A mode the DCM (Door Control Module) is placed in, in the unlikely event it becomes “disconnected” from the rest of the PassPoint system. In this mode, the DCM can be told how to operate while it is out of contact with the MLB (Main Logic Board).

**Reader** - A device that a cardholder presents his access card to, that reads the card’s encoded data and transmits it to an access control panel. The panel then makes a decision as to what action to take as a result of that card read (energize a relay, etc.).

**Relay Supervision** - The monitoring of the common pole of the Form C relay for the presence of voltage. An alert is generated if the voltage is not sensed. This might be used to determine whether 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)** - A function that disables the DSM zone on the access point. The access point then operates 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)** – A function that serves almost the same purpose as the Bypass Zone function, with 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 remain shunted until it is repaired.

**Skeleton Codes (or Skeleton Cards)** - Codes that 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** – A feature that grants access to a cardholder in violation of anti-passback rules, but records the violation in the event history.

**Soft Entry/Exit** – A feature that grants access to a cardholder in violation of entry/exit rules, but records the violation 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 that 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** - Solid state digital switches (transistors) that can be configured as committed or uncommitted resources. These can be used to illuminate LEDs, activate piezoelectric sounders, energize an external relay, or signal a long-range radio transmitter.

**Trouble** - A condition that generally indicates a problematic line (cable or connection) for a supervised zone.

**TWAIN** - A program that lets you scan an image (using a video camera or scanner) directly into the application where you want to work with the image. This may be used for tasks such as inserting photo IDs into the PassPoint *Plus* employee files.

***U***

**User (system)** - A person who 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.

**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 resets the control electronics in the unlikely event that it becomes locked in an endless loop of some kind. This allows the system to continue to operate even though there is usually a problem that would otherwise 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 cardholder.

**Windows (Time)** - A time interval during a 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.





## Index

# I

## *Access Control Index*

ABA MagStripe Cards.....	7–8	Custom Tab.....	6–18
Access Starter Kit .....	1–2, 1–6	Employment Tab .....	6–17
Account		Events Tab .....	6–23
Create New .....	4–9	Managing .....	6–1
What is? .....	4–10	Monitor .....	6–33
Adding a CEK .....	10–1	Personal Tab .....	6–16
Adding a DEK .....	9–1	Summary Tab.....	6–20
Adding a VGM.....	11–1	CEK	
Adding Cardholders.....	6–2	Adding .....	10–1
Adding System Modules.....	12–1	Configure Reader.....	10–12
Auto Enroll Modules .....	5–9	Connecting.....	10–3
Basic Starter Kit.....	1–2	Downloading Database .....	10–15
Bulk Edit Cards .....	6–24	Editing Configuration .....	10–12
Card Enrollment Kit .....	1–2	Enrolling .....	10–5
Card Monitor .....	6–33	Installing .....	10–3
Card Wizard.....	6–4	Understanding.....	10–2
Cards		Communications, Connect.....	5–7
ABA MagStripe.....	7–8	Computer System Requirements.....	4–5
Access Tab.....	6–10	Configuring DCM.....	9–20
Action Tab .....	6–14	CPM Setup.....	12–17
Add Batch.....	6–9	Create New Account.....	4–9
Add Single .....	6–5	Database	
Adding Manually .....	6–9	Cardholder, About .....	6–2
Bulk Edit.....	6–24	Cardholder, Managing .....	6–1
Custom Fields Tab.....	6–19	Cardholders, Adding.....	6–2



Download .....	5–13, 9–19, 10–15, 11–22	Connect Door Strikes .....	3–11
DCM .....	1–8	Connect Magnetic Locks .....	3–11
Access Point A Tab .....	9–22	DCM/MLB Connection .....	3–6
Access Point B Tab .....	9–22	DCM/Power Supply Connection .....	3–6
Configuring .....	9–20	DEK .....	9–3
Connecting .....	9–5	DSM Connection .....	3–12
Editing Configuration .....	9–20	Hardwire Computer Connection .....	3–13
Enrolling .....	9–8, 9–14	Keypad Connection .....	3–18
MLB Connection .....	3–6	MLB RS-232 Ribbon Cable Connection ...	3–7
Power Supply Connection .....	3–6	MLB/Power Supply Connection .....	3–6
Readers Tab .....	9–35	Mount Door Strikes .....	3–11
Relay Tab .....	9–36	Mount Magnetic Locks .....	3–11
Skeleton RCM Tab .....	9–43	Mount System Panel .....	3–4
System Tab .....	9–22	PassPoint <i>Plus</i> .....	4–7
Triggers Tab .....	9–38	Remote Computer Connection .....	3–15
Zones A/B Tab .....	9–40	RTE Connection .....	3–12
Zones C/D Tab .....	9–40	System .....	3–1
Defining Resource Lists .....	8–2	System Power Up .....	3–18
DEK .....	1–2	VGM .....	11–3
Adding .....	9–1	Installation, Preparing for .....	2–1
Installing .....	9–3	Card Reader Types .....	2–15
Mounting .....	9–3	DCM Configuration .....	2–13
Understanding .....	9–2	Door Control Hardware .....	2–4
Door Control Module .....	1–8	Floor Plan .....	2–5
Door Expansion Kit .....	1–2	Selecting Access Points .....	2–8
Download		Understanding access points .....	2–3
MLB Firmware .....	B–1	Kit	
Download Database ....	5–13, 9–19, 10–15, 11–22	Access Starter .....	1–2, 1–6
Enroll		Basic Starter .....	1–2
CEK .....	10–5	Card Enrollment .....	1–2
DCM .....	9–14	Door Expansion .....	1–2
Modules, Auto .....	5–9	Logical Window .....	4–14
System Modules .....	12–3	Main Logic Board .....	1–8
VGM .....	11–6	Menu Bar .....	4–14
Event Window .....	4–14	MLB .....	1–8
Firmware		Power Supply Connection .....	3–6
Download .....	B–1	RS-232 Ribbon Cable Connection .....	3–7
Installation		MLB Connections .....	A–9, A–10
Card Reader, Connecting .....	3–7	MLB Mounting .....	3–4
Card Reader, Mounting .....	3–7	Modules	
CEK .....	10–3	Auto Enroll .....	5–9

PassPoint <i>Plus</i>	
Event Window .....	4-14
Installation .....	4-7
Logical View Window .....	4-14
Login .....	4-8
Major Screen Components .....	4-13
Menu Bar .....	4-14
Priority Bar .....	4-14
Quick Finder .....	4-14
Resource Control Tool Bar .....	4-14
Resource Window .....	4-14
Speed Buttons .....	4-15
Starting .....	4-8
Status Area .....	4-14
Power Supply .....	1-8
Power Supply Specifications .....	A-11
Priority Bar .....	4-14
QRM	
Editing Configuration .....	12-10
QRM Setup .....	12-12
Quick Finder .....	4-14
Resource Control Tool Bar .....	4-14
Resource Lists	
Defining .....	8-2
Using .....	8-11
Resource Lists .....	8-1
Resource Window .....	4-14
Setting System-Wide Options .....	7-1
Setup Wizard .....	5-4
Software Setup .....	4-1
Speed Buttons .....	4-15
Starting PassPoint <i>Plus</i> .....	4-8
Status Area .....	4-14
System Hierarchy .....	1-3
System Installation .....	3-1
System Interface .....	1-9
System Modules	
Adding .....	12-1
Adding and Enrolling .....	12-3
Configuring .....	12-10
CPM Setup .....	12-17
Downloading Database .....	12-24
Installing .....	12-3
QRM Setup .....	12-12
Understanding .....	12-2
ZIM Setup .....	12-21
System Panel, Mounting .....	3-4
System Requirements, Computer .....	4-5
System-Wide Options .....	7-2
Access Point Beep/Video Tab .....	7-32
Burg System Tab .....	7-28
Card Tech Tab .....	7-6
Dialer Reports Tab .....	7-33
Modem Tab .....	7-33
Network/ID Tab .....	7-36
Presets Tab .....	7-3
Priorities Tab .....	7-38
Setting .....	7-1
Skeletons Tab .....	7-16
Using Resource Lists .....	8-11
VGM	
Adding .....	11-1
Configure .....	11-13
Connecting .....	11-4
Downloading Database .....	11-22
Editing Configuration .....	11-13
Enrolling .....	11-6
Installing .....	11-3
Wiring Considerations .....	A-1
DCM Connections .....	A-10
MLB Connections .....	A-9
Power Supply Specifications .....	A-11
Topology .....	A-2
Wire Characteristics .....	A-8
Wiring Notes .....	A-7
Wiring Reference .....	C-1
Wizard	
Card .....	6-4
Setup .....	5-4
ZIM	
Editing Configuration .....	12-10
ZIM Setup .....	12-21







5007 South Howell Avenue  
Milwaukee, WI 53207  
[www.nciaccess.com](http://www.nciaccess.com)

Copyright © 2000 PITTWAY CORPORATION



K4879 03/00

**ADEMCO**  
**GROUP**  
INTEGRATED SYSTEMS





5007 S. Howell Avenue, Milwaukee, WI 53207 • 1-800-323-4576  
[www.nciaccess.com](http://www.nciaccess.com)



K4879 3/00

**ADAM**  
**GROUP**  
INTEGRATED SYSTEMS