SE 6000

SECURITY MANAGEMENT SYSTEM

STANDARD PRODUCT MANUAL

Westinghouse Security Electronics
an ISO 9001 certified company

5452 Betsy Ross Drive
Santa Clara, CA 95054-1184
(408) 727-5170
FAX (408) 727-6707

P/N 66107919001, Rev. F

LIMITED WARRANTY

Westinghouse Security Electronics (WSE) warrants to the original user the equipment manufactured by WSE as described herein (the equipment) to be free from defects in material and workmanship for a period of one year from the date of purchase by such user or fifteen (15) months from the date of shipment from the factory, whichever is sooner, provided:

I WSE has been notified within such period by return of any alleged defective equipment, free and clear of any liens and encumbrances to WSE or its authorized Dealer at the address specified, transportation prepaid; and

II the equipment has not been abused, misused or improperly maintained and/or repaired during such period; and

III such defect has not been caused by ordinary wear and tear; and

IV such defect is not a result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war or similar phenomena; and

V accessories used as an integral to WSE systems have been approved by WSE (e.g., coaxial cables, batteries, etc.); and

VI the equipment has been installed, the installation supervised or installation tested by an authorized WSE dealer.

WSE's Proximity Command Keys are warranted for 5 years. WSE shall at its option, either repair or replace, free of charge, the equipment found, upon WSE's inspection to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the equipment. Magnetic Stripe Cards are warranted as described by the manufacturer's warranty.

WSE makes no other warranty, and all implied warranties including any warranty of merchantability or fitness for a particular purpose are limited to the duration of the expressed warranty period as set forth above.

WSE's maximum liability hereunder is limited to the purchase price of the equipment. In no event shall WSE be liable for any consequential, indirect, incidental or special damages of any nature arising from the sale or use of the product.

Some states do not allow limitations on incidental or consequential damages or how long an implied warranty lasts, so the above limitations may not apply. This warranty gives specific legal rights; however, other rights which vary from state to state, may pertain.

IMPORTANT

The information provided in this manual is believed to be accurate and reliable. However, Westinghouse Security Electronics (WSE) assumes no responsibility for any errors that may appear. Possession of this manual does not imply the granting of licenses to make or sell equipment or software constructed according to descriptions provided.

TABLE OF CONTENTS

SECTION 1
INTRODUCTION

MANUAL ORGANIZATION

This manual follows the order of the seven standard product items in the system main menu, with the *Key Inventory* and *Parking Stickers* items merged into the *System Administration* section:

- *Section 2: Monitor Security Activity*
- *Section 3: Security Management Reports*
- *Section 4: Master File Entry*
- *Section 5: Master File Reports*
- *Section 6: System Administration*

System Main Menu

The system main menu is the departure point for accessing all other system screens (main menu screens may vary according to options purchased).

Documentation Methods

To avoid repetition and to reduce document size, detailed explanations for the system's principal data items are given only in *Section 4: Master File Entry*, which is used when creating the system database. For introductory information concerning the data items, see *Definitions* below.

Further, with the exception of the screens presented in *Basic System Usage* in this section, and the introductory menu screens for *Sections 2* through *Section 5*, all other screens throughout this manual are limited to the particular screen area being discussed (i.e., full screens are not shown). In some cases, screen presentations are unnecessary and are not used.

DEFINITIONS

General

Access Code. A group of readers and time codes assigned to keyholders indicating where and when entry is permitted. Note that access codes can be associated with a down loadable device ID for distributed processing or they can be associated with the host computer for central processing.

Access Group. A group of access codes created to facilitate the assignment of similar access privileges to a large number of keyholders.

Alarm Contact. A dry-contact switch, indicating input conditions for smoke detectors, heat / moisture sensors, taut-wire fences, window bands, etc.

Company. Keyholder's employer.

Department. A particular group within a company to which a keyholder is assigned.

Device. A controlling element of the system which communicates with the computer and the system points (see *System Hardware* in this section).

Event. Any defined transaction which requires action by an access control system. Examples: keyholder entry request, activated alarm.

Job Category. A code assigned to a keyholder indicating the employee group category.

Key Number. Keyholder's security key number. Unlike the keyholder ID, this number may be changed (e.g., if a key is lost) or removed (e.g., if an employee leaves the company).

Keyholder. Employee or visitor who holds a valid security card for an access control system.

Keyholder ID. Keyholder's ID number. The unique ID number is used by the computer to keep track of all activity for that person. Once entered, the keyholder ID cannot be changed.

Location. Location of the office or branch of the company to which a keyholder is assigned.

Tenant. One of several distinct occupants of a facility with a single access control system. The data for each tenant using the system appears separate from that of all other tenants.

Time Code. A definition of the time of day, and the days of the week, when events are to occur. Used in assigning access privileges, performing scheduled tasks, and monitoring points.

Trace. A realtime (as it is happening) display of events for a specific keyholder or point.

Transactions. System responses to events are called transactions. The most frequently seen is ACCESS GRANTED, which means a valid key was presented to a reader at an approved door, at an approved time, and that the keyholder was granted entry.

Zones. Selected locations and device types may be grouped into zones to facilitate system control. For reporting purposes, zones may be grouped into areas. If zones are created, anti-passback instructions or controls may be assigned (see *Access Control Functions* in this section).

System Hardware — Devices

The principal device is the host computer. The host controls all data maintained in the database, records all system activity, and is the central point for all reporting activity. The host communicates with all system devices, or may communicate via an LC or RLC computer (see *Optional Features* in this section).

Various other devices are included in access control systems. Simple systems may use only contact switches and a single reader type. More complex systems may use several reader types and many other devices. Devices are classified as input or output units depending on their particular function. Input devices are detectors and identifiers; output devices are alarms and control units.

Devices — Microprocessor Units

Access Control Units (ACUs). In conjunction with the host or local computer, the ACUs are used to control door access and maintain status. Example ACUs are: WSE NexSentry, 422, 708P, and 8xx-series. The WSE 708P units are called simple devices because they do not make access decisions (decisions are made by host). The NexSentry, 422, and 8xx-series units are called intelligent devices because they can make access decisions independent of the host.

Biometric Hand Readers. Devices such as fingerprint analyzers, hand geometry analyzers, retina scanners, and other devices which check body characteristics.

Readers

Digital Key Reader. Reads the unique number of 1 to 5 digital command keys simultaneously at a range of up to 36 inches.

Keypad Controllers. The keypad controllers, normally used in conjunction with an ACU, provide additional security by requiring a personal identification number (PIN) entry.

Magnetic Card Readers. Reads the card number from information coded into the magnetic strip on the card. Card must be moved physically through the reader to work.

Readers (also called Sensors). These units electronically read the security key presented and transmit the data to the ACU. Three reader types are used: Proximity; Magnetic Stripe; Wiegand.

Inputs

Alarm Contacts. These devices monitor simple contact inputs, and control outputs and switches with contact closures for alarm monitoring, elevator control, camera switching, and other tasks.

Contact Alarms. Simple dry-contact switches indicating if a contact is open or closed.

Door switches. The computer controls only the lock power to the door, and the door switches are the contact points which inform the computer whether a specific door is open or closed. Each door switch is assigned to a specific reader.

Fire Alarms / Heat Sensors. Data from smoke detectors and heat sensors can be sent to the computer to alert it to alarm conditions. Although fire alarm systems are generally separate from access control systems, the computer can be used to provide enhanced response capabilities.

Intrusion Devices. Taut wire fence, infrared detectors, field-disturbance detectors and other device types can alert the computer to the presence of personnel in unauthorized areas.

Motion Sensors. Detect physical movement in an area. Can be used to tell the computer that someone wants to exit (go through a door from the uncontrolled side), or to protect secure areas.

Video Monitor Switchers. The computer routes the signal from a particular video camera to a specific monitor based on conditions in that area. For example, if the computer detects an open rear door, it can display the camera output at that door on the terminal at the security desk.

Multiple Switch Monitor (MSM). The MSM is a four-contact switch box that is connected to a WSE ACU and the MSM provides four contact-closure inputs.

Points. A point is any basic element of an access control system, such as a door switch, an alarm contact, an output switch. Point IDs uniquely identify all system elements.

Request-to-Exit (REX) Sensor. Used when both entry and exit control is required. REX points, usually push-button devices, motion detectors, or push-bars, tell the computer that someone inside a building wants to exit. The computer needs to know this to unlock the door, or to disregard the door opening as being an alarm event.

Outputs

Audible Alarms. The computer can trigger bells, buzzers and other types of audible alarms.

Remote Alarms. The computer can dial police and / or fire departments, or any other agency, as part of an alarm response plan.

System Software

The system software links all input and output elements. The software collects and reports data from input devices, and controls the output devices based on this information. The software also detects and reports any hardware problems that may occur.

Complete Portability. A specific computer type is not required, although Hewlett-Packard computers are preferred because of performance and worldwide service. Application programs run under an SCO / UNIX operating system.

Installation Flexibility. The SE 6000 can control many hardware setups, including remote site networks. The system can be programmed to control data flow between central and remote computers to create a large-size security system controlled from a central point.

Integrated Software Support. The SE 6000 communicates with a variety of access control and alarm monitoring devices. Currently, the system interfaces with WSE ACUs and their peripheral devices, alarm multiplexers produced by Stellar Systems and Optomux, magnetic stripe readers, CCTV camera switchers made by Burle, Pacom, American Dynamics, and Vicon, Radionics alarm panels, and Recognition Systems hand geometry readers. In addition, the system supports communication with the WSE 8xx-series ACUs over dial-up telephone lines using a remote dial-up interface (RDI) device. The ID-4000 badging system includes options for badge designs on film or on PVC.

Open System Design. There are few restrictions on the number of security keys, key readers, or other system elements used with the SE 6000. Increasing system capacity only involves upgrading the computer power by adding more memory or disk space, or installing a faster processor. This means that, as a company grows, it cannot outgrow the SE 6000.

Response Time. The SE 6000 is capable of fast response times in both single and multiple site configurations. Fast response times are important for security personnel who monitor alarms and are always appreciated by keyholders wishing to enter locked doors.

Principal System Functions

Access Control

Anti-Passback Control. The SE 6000 has anti-passback features (applies to zones only) to prevent tailgating or unauthorized key use. Anti-passback is possible across multiple access control devices, and can be hard (denies access) or soft (allows access, but displays and logs a message). The software handles vehicle and personal passback separately.

Automatic Access Control. Permits employees or visitors with assigned access codes to pass through only those doors assigned to them and only during the proper days and hours.

Automatic Activate / Deactivate. Permits the automatic activation of specific output points to control lighting, status indicators, or other electrically controlled functions.

Automatic Unlock / Lock. Allows doors to be opened automatically only during specified time periods, then re-locked automatically at a later time.

Communications Monitor. Permits security personnel to check all wiring and communications to all hardware elements and displays raw data exchange between the host computer and a connected device.

Event Monitoring. Displays events as they occur and monitors the door status and other access points. Allows security personnel to watch events at all doors in the system from one location.

Flexible Event Handling. Flexible event handling automatically activates outputs, displays special messages, and enables / disables devices. Anything which can be done manually on the SE 6000 can also be performed automatically using this feature.

Independent PIN Entry. Access control can be enhanced using personal identification numbers (PINs). PINs are entered via keypad devices assigned to readers. Also, high-security independent devices (hand geometry readers, e.g.) can identify the user.

Manual Access Control. Allows security personnel to manually open any door in response to an access request. May be used with closed-circuit TV to verify and admit people, or to track keyholders who have forgotten their keys. Includes the capability to record keyholder IDs if keys are not available. All manual actions are logged as events.

Two-Man Rule. The SE 6000 can be programmed to grant access only after two valid key presentations have been made at the same reader within a predefined period of time.

Multiple Occupancy Feature. Similar to the two-man rule except that it requires that two keyholders enter and leave a specified zone together; refer to Section 4 for details.

File Maintenance

To perform its access control functions, the system must know the unique ID numbers of all keyholders and the doors and times they can enter. Further, the SE 6000 maintains other keyholder data to facilitate scheduling and reporting.

The system also needs to know details of the location of input devices and other security hardware. File maintenance functions allow users to enter, modify, or delete employee, company, physical connection and time information, as required.

Reporting

The SE 6000 produces a comprehensive selection of reports for display at the system terminal or for hard-copy output from the system printer:

Alarms and Responses. A history report of alarms which occurred at a specific time and location, and the responses taken by the security staff.

All Transactions. A report detailing all system activity. The items reported can be limited to specific information items.

Database Changes. A report of database change activity, which includes the name of the operator who made the changes. Note that this requires that the journaling feature be enabled.

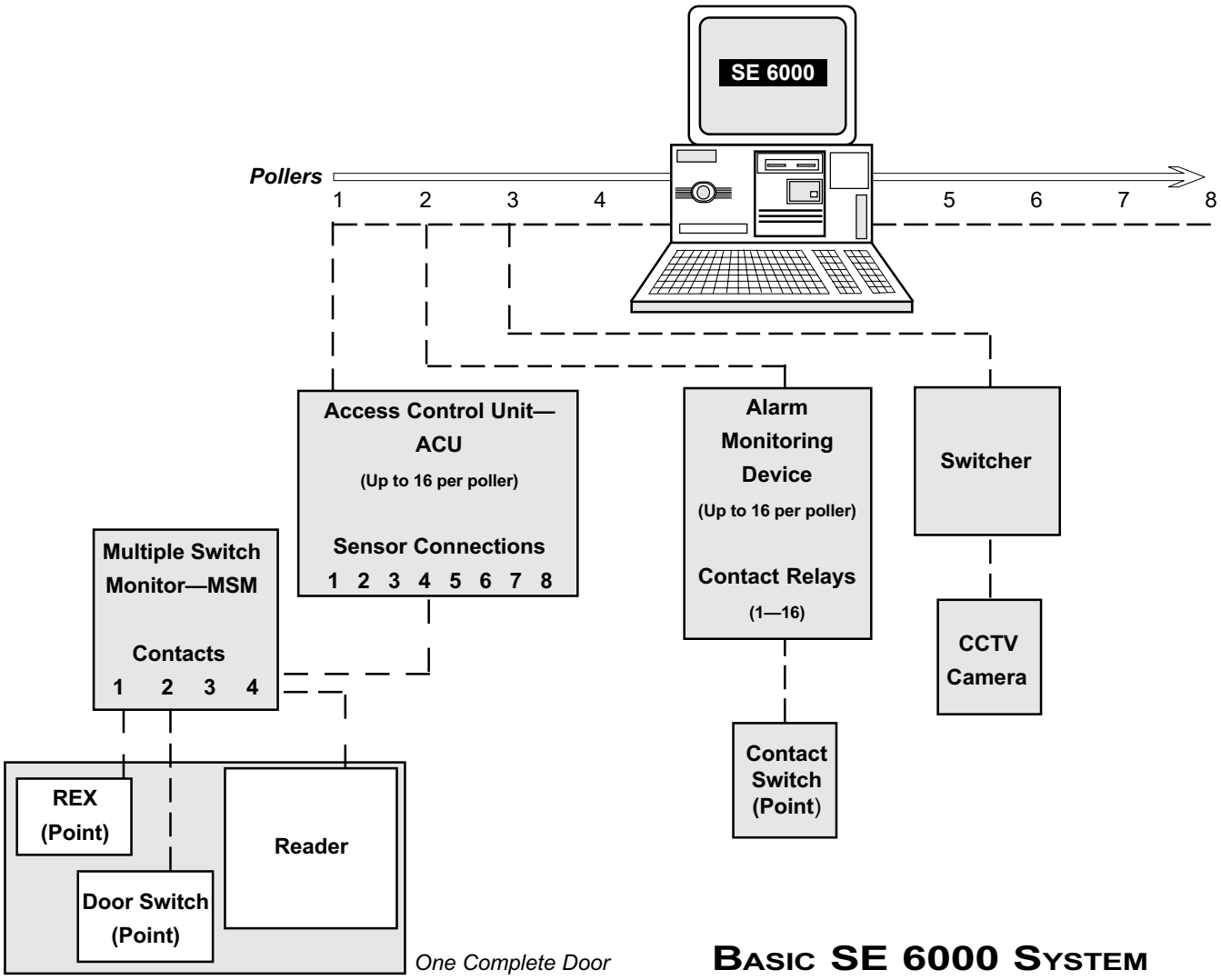
Invalid Access Attempts. A report detailing events which were not valid accesses during specific time periods at particular doors.

Keyholder History. A report of the last twenty uses from a particular keyholder.

Point History. A report of the last twenty events at any door or point. Designed as a quick way to view a limited number of events. Additionally, reports can be created which provide information about the keyholders in the system, access privilege definitions, company information, input devices, and other subjects.

SAMPLE SYSTEM

An illustration of a basic SE 6000 system follows:



BASIC SE 6000 SYSTEM

CREATING THE DATABASE

Once the system is in place, first obtain the following from the system installer:

System Interconnect Diagram. This shows all wiring and connections in the system, and provides information needed for entering pollers, devices, readers, and points.

Poller Initialization Parameters Information. The information shows how the pollers were initialized, including poller type, physical port connection, and other poller-specific information. Because all system activity is based on four-digit ID numbers, you need to decide before data entry how these numbers are to be assigned to the system hardware elements. Although the numbering system is entirely the choice of the SE 6000 owner, we recommend one of the two following methods:

1. Following the *System Interconnect Diagram*, number each element in turn with a four-digit number, including numbers for devices, pollers, and readers.

2. Use the following ID groupings for average-sized system:

0001-0010	—	Computers	2000-2999	—	Door switches
0011-0099	—	Pollers	3000-3999	—	REX contacts
0100-0999	—	Devices	4000-5999	—	Input points
1000-1999	—	Sensors	6000-7999	—	Outputs

Data Entry Sequence

Note that although the zoom feature (described later in this section) permits faster data entry, WSE recommends the following sequence for most efficient data entry when you are creating your database (data entry is detailed in *Section 4: Master File Entry*):

1. Time Codes
2. Tenants
3. Zones / Areas
4. Pollers
5. Devices
6. Points
7. Readers
8. Access Codes
9. Access Groups
10. User-Defined Fields
11. Keyholders
12. Access Privileges
13. Holidays
14. Alarm Instructions
15. Maps
16. Transactions
17. Tasks
18. Events
19. Enable Terminals for Global Alert
20. Program Security Levels
21. Add Users
22. Passwords
23. System Owner Name
24. Terminals for Alarm Auto-Switch

NOTE

Consult the system installer if you have questions concerning numbering. In any case, keep track of your numbering method and advise each operator of the method selected

BASIC SYSTEM USAGE

This subsection gives introductory information for using the SE 6000 system, and includes related miscellaneous information.

Logging On

Power on the system terminal. The screen displays a brief welcome message followed by the *login* and *password* prompts. Enter the login ID and password in lowercase letters. If uppercase letters are entered by mistake, log off using uppercase letters then log on again with lowercase letters.

If the login and password are not valid or if one or both were not entered correctly, the computer responds with *login incorrect* then displays *login* again. Reenter the login ID and password making sure that each letter is correctly typed. If the *login incorrect* message continues, consult the system administrator. When logged in correctly, the system displays the SE 6000 title page, sets the terminal environment, then displays the main menu. Call WSE Customer Service if you have a login problem.

System Screens

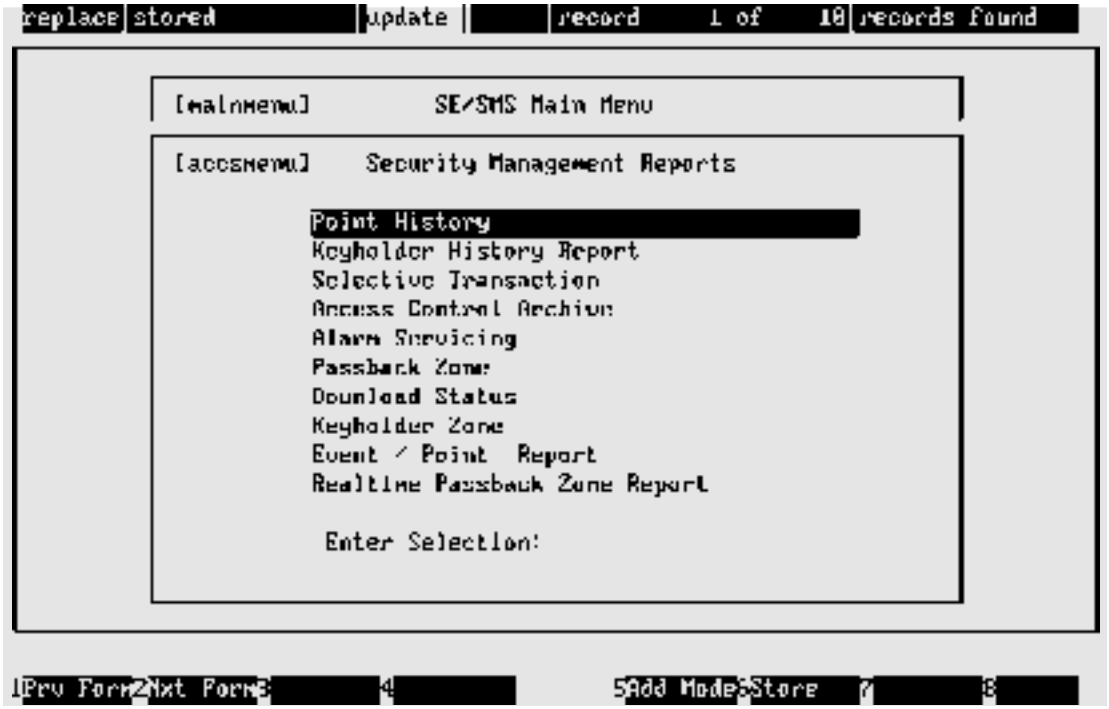
There are two basic screen types: *Menu* and *Application*:

Menu Screens

Menu screens list application selections by group according to function (exception Monitor Security Activity — see Section 2). All menu screen IDs end in ***menu*** (example: [fmntmenu] — Master File Entry).

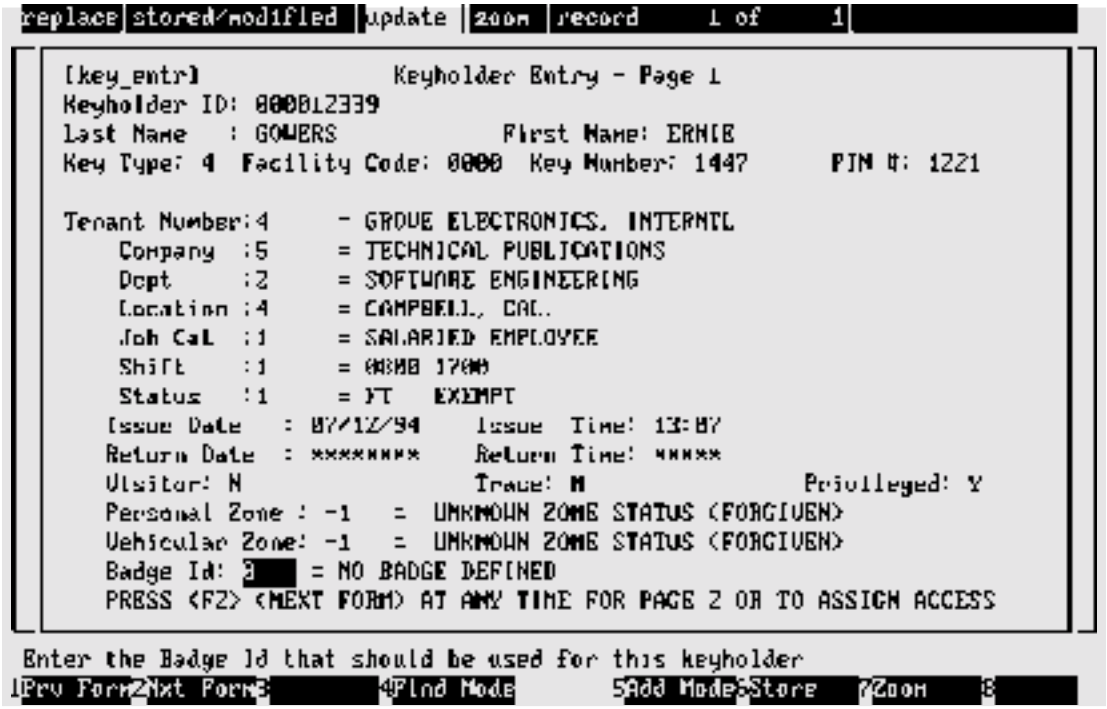
The menu screens have three elements: the list of choices, the highlight bar, and the *Enter Selection* field. The highlight bar, controlled by the arrow keys, is used to make a selection to be placed into the *Enter Selection* field. Screen access descriptions are given in *Moving Between Screens and Fields* in this section.

A sample menu screen follows:



Application Screens

Application screens use status windows and various fields for entering new data or displaying existing data. The screen title is in brackets and on the same line and to the left of the screen title. Most screen title IDs indicate screen function, e.g., ***entr*** (enter data), ***rprt*** (report). A sample screen follows:



Indicates *replace* or *insert* mode. With *replace*, entries overwrite existing data. With *insert*, entries push existing data to the right. Toggle between the modes by pressing *insert*.

Indicates if the information displaying is stored.

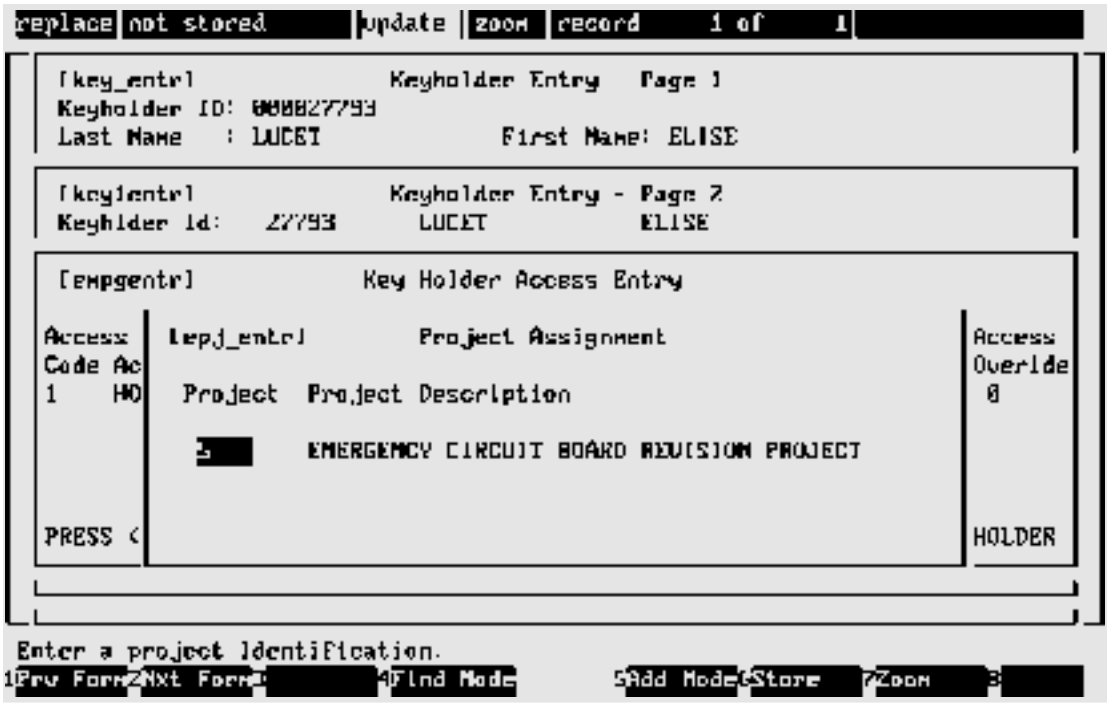
Indicates the current screen mode (see *Finding, Adding, and Storing Data* in this section). In some systems, this window is in reverse video.

Indicates if the zoom feature exists for a field (see *Zoom Feature* in this section).

Displays the number of records found as a result of a *find* request (*see Finding, Adding, and Storing Data* in this section).

SCREEN EXAMPLES

SE 6000 screen displays show the path used to access the screen. For example, the final screen used when setting up keyholders, [epj_entr], is accessed via three preceding keyholder setup screens: [key_entr], [key1entr], [empgentr]. This useful feature considerably assists the new SE 6000 user when becoming familiar with the system. A sample [epj_entr] screen follows:



USING SCREENS AND FIELDS

Selecting Screens

There are three screen selection methods:

1. Use the arrow keys to select the menu choice. Press Enter to place it in the *Enter Selection* field, and press Enter again to display the selection.

2. Use the arrow keys to select the menu choice, and press F2 to display the selection.

3. Press Enter anywhere in the list of choices to move the highlight bar to the *Enter Selection* field. Press Ctrl + y to clear the field and type the title of the screen required and then press Enter.

Moving Between Data Fields

Move between the application screen data fields as follows:

- To move forward through the fields, press Enter.

- To move backward through the fields, press Ctrl + u.

- To move between characters within a single field, use the left and right arrow keys.

Moving to Prior Screens

Press F1 to return to the previous screen displayed. If required, continue to press F1 to return to the system main menu.

FINDING, ADDING, AND STORING DATA

Finding Data

Use the find mode to locate and select data. A specific record (a single keyholder ID, for example) or a group of records (all keyholders in a particular job category, for example) can be found.

For example, assume we need to find all keyholders assigned to tenant 2 who began work after May 1, 1995. First, select the keyholder entry screen, [key_entr]:

NOTE

The *keyholders* are the object of the search, which is why we begin at the keyholder entry screen. *Tenant 2* and *issue date* are the search criteria.

1. Press F4 to clear fields and to enter the find mode. The third status field at the top of the screen displays *find*.

2. Press Enter to advance the highlight bar until you reach the first search item, *Tenant*, and type 2.

3. Press Enter to advance the highlight bar until you reach the second search item, *Issue Date*, and type *05/01/96*. (Note: Enter the date according to the format for your system, that is, either MM/DD/YY or DD/MM/YY.)

4. Press F3 to begin the search process; the sixth status field displays *finding*. The length of the search process will depend upon the size of the data base.

5. When the search completes, the system displays the first record found and shows the number of records found in the fifth status window (*Record 1 of* n). (If the system doesn't find any records matching the search criteria, the message *No Records Found* displays.)

   Use the down arrow key to display other records found in the search process. Use the up arrow key to go back to previous records.

Searching With Partial Information

Records can be found using partial information. For example, to find all keyholders whose last name begins with T, enter T in the *Last Name* field. The system also searches for several criteria. For example, to find all keyholders who work for tenants 1 and 5, enter *1,5* in the *tenant* field. In addition, you can enter less than (<) and greater than (>) symbols to narrow a search.

The computer automatically changes to the update mode when a search completes, and the records selected can be updated if required. To start another search, press F4 to clear the screen and begin again.

Adding / Changing Data

The add mode is used to input new records. Once a record is found using the search mode, update is automatically selected which allows the user to change the existing data.

If not already in the add mode, press F5 to clear fields and to begin adding. Press Enter to move the highlight bar to the next field and type the data. (If a typing mistake is made, press Ctrl + y to clear a field, Ctrl + f to delete characters in a field, Ctrl + u to move back through the fields.)

Many fields have default values, which are used if a field entry is not made. Default values are used to simplify the entry process by automatically setting certain fields to commonly used values. For example, many yes or no type fields, (Y / N), have Y as the default.

Storing Data

Store all additions and changes when completed — Press F6. If F1 is used to return to the previous screen without first storing the new / changed information, all the new data is lost.

DELETING RECORDS

From time to time, it may be necessary to delete records from the database. The delete record function is easy to perform, although some cautions are involved. To remove a record from the database, first display the record using the find mode, then press Esc, followed by *d* (lowercase), then *r* (lowercase). If the operation can be performed, the computer displays *deleted*.

It may not be possible to delete records in some cases. For example, the system would not allow a reader to be deleted without first deleting its associated access codes. Display the access code records and delete the reader data appearing on them, then delete the reader record itself again.

CAUTION

Be careful when deleting certain records. For example, it is unwise to be hasty when deleting keyholder records. Consider Employee A who occasionally entered a certain room where valuable material is stored. The employee then abruptly left the company, and the keyholder record is deleted. A theft is then discovered from the room, and from shipping and receiving records it is determined that the theft occurred within a particular time frame. But with the keyholder information now erased for Employee A, there is no way to link the transaction history to a particular keyholder.

ZOOM FEATURE

The *zoom* feature provides a fast method for accessing linked or dependent application screens and for copying data from these screens to other application screens. When the feature is available, *zoom* displays in the status bar.

For example, you are entering keyholder data (keyholder entry screen) but don't know the tenant code for the keyholder. When in the *tenant* field, press F7 to *zoom* to the tenant entry screen. Once there, use the find mode to see the tenant codes defined and to select the one you need or enter a new one. Then press F1, and the system automatically returns you to the keyholder entry screen and enters the keyholder's tenant code in the *tenant* field.

Cancel Zoom

If you don't need data from the *zoom* screen, press *Esc*, then Ctrl + z to return to the previous screen, or simply return using F1 and key over the returned data.

MISCELLANEOUS INFORMATION

- If you need help in any field in the system, check the instructions on the information line at the bottom of the screen.

- If the computer beeps and displays a message, or if you see the symbol '---' in the information area at the bottom of the screen, press Enter to let the computer know you've read the message. The computer will not allow further action, and will beep each time you press a key until you press Enter to acknowledge.

- Occasionally, a screen will not display properly. This can occur when accessing the system from a remote dial-in terminal via a modem or when the system administrator sends a message. If this happens, try using Ctrl + r to redraw the screen. To completely clear the problem, log off the system and log on again.

- To save time when moving around the SE 6000 system, it pays to learn the screen titles of the most commonly used application screens (see the screen location trees and the table at the end of this section). For fast screen access, type a screen title in the *Enter Selection* field (press Enter in any menu screen), then press Enter and the system immediately displays the screen. Note that you should delete any characters remaining in the *Enter Selection* field before you select Enter.

LOGGING OFF

When the SE 6000 session is completed, press F1 until you reach the main menu screen. From here, press F1 again; the computer asks for log off confirmation. Enter yes (full word) and press Enter to leave the system. (You can also type exit in any Enter Selection field to leave the system.) After log off, the computer displays the login prompt again.

IMPORTANT

Log off the SE 6000 system formally before you leave the terminal. If you do not log off, any action taken by the next person at the terminal will appear under your name.

SHUTTING DOWN

Always use the following procedures, in the order given, when powering off the SE 6000:

1. Go to the main system terminal (system console). This terminal has overall computer control and displays all system messages.

2. Log off the system using the procedures given in the previous subsection.

3. Log in using the SHUTDOWN login. Your system administrator will provide you with the password. If other users are still logged on, you may have to press Enter to continue the shut down process which will forcibly log off other users.

Step 3 automatically shuts down the SE 6000 system in an orderly way. The last message displayed when the internal shutdown procedures have completed is *Safe to Power Off* or *Press any Key to Reboot*. It is now safe to power off the computer. To restart the computer, press any key and follow the instructions in the following subsection.

RESTARTING

Use one of the following methods, *Automatic* or *Manual*, when powering on the SE 6000 (the shutdown / restart process is also known as *rebooting* the computer).

Automatic Restart

The SE 6000 has an automatic restart capability that reboots the system in the event of a power interruption. If unattended, the *Boot* prompt displays for 30 seconds, then the auto-boot function reloads the operating system and restarts the application including the pollers.

Manual Restart

1. Turn the power on; the computer displays *Boot.* Press Enter to continue.

2. After various messages, the computer displays *Type Control-d to Proceed with Normal Startup (or give root password for system maintenance***)**. Press and hold the Ctrl key, and press the *d* key (lowercase).

3. The computer displays *Enter new time ([yymmdd]hhmm).* Change the date and time values as required (do not enter the parentheses or brackets); press Enter when completed. To keep the displayed date and time, press Enter.

4. The computer continues its startup procedures, and the *login* prompt displays after a brief pause. If any other message displays apart from those noted here, just press Enter.

SYSTEM SCREEN TREES

The SE 6000 screens are arranged in tree structures, with hierarchies established from the primary screen to the lowest level screens in each tree. Each screen has a unique title which displays in the upper-left.

Appendix A: System Screen Trees

Tree structures for the first seven standard-product selections on the system main menu are given in *Appendix A*:

- Monitor Security Activity
- Security Management Reports
- Master File Entry
- Master File Reports
- Key Inventory / Parking Stickers
- System Administration

Appendix B: System Screen Hierarchies

Appendix B lists all screens within their respective tree structures, along with a brief explanation for each. Left column indentions show the relative position of each screen within the individual tree structures. Indented screens can be accessed only from the previous level in the screen hierarchy.

OPTIONAL FEATURES

A variety of optional software packages are available with the SE 6000:

IQ. A report writer package that allows the user to select, sort, display and / or print database information in a format specified by the user. It can be used for quick ad hoc enquiries or formal reports. Once defined, report formats may be saved and rerun on demand.

CCTV Camera Switcher Control. Controls the actions of closed-circuit television system switchers, allowing the system to switch video output from a particular camera to a specified monitor. When used in conjunction with the system flexible event handling feature, this provides an important method for monitoring system events.

Controller Systems. Controller systems are computers running the SE 6000 local (LC) or remote location controller (RLC) software. The LC system is a computer attached via dedicated lines to the host. The RLC system is a computer attached via dial-up telephone lines to the host.

Elevator Control. Permits floor-by-floor control of elevator call buttons. When a keyholder presents a key to a reader in the elevator, certain buttons, wired via computer-controlled output contracts, can be enabled or disabled for use. The keyholder is able to select only those which have been enabled for his / her specific access privileges.

Guard Tour. Schedules and monitors security personnel guard tour activities. Specifies certain reader output points as guard tour points, and assigns the minimum and maximum times which can pass between stops on the tour. The feature reports if tours have started too early or too late, or if too little or too much time has passed between stations.

Parking Control. Controls and monitors a parking facility including employee and revenue generating parking spaces. Includes keyholder and daily cash customer functions, tenant billing, and overage features. Supported hardware includes point-of-sale terminals, automated ticket dispensers, and gate control mechanisms. Produces detailed reports for keyholders, cash customers, parking lot attendant activity, and keeps track of the number of cars in the lot on a tenant-by-tenant basis.

Remote Dial-Up Interface (RDI). Permits communication with remotely-located 8*xx*-series devices via dial-up telephone lines. The feature retains transaction information, and determines when conditions at a remote site warrant a call to the host (alarm event occurring, log buffer reaching a user-defined threshold, etc.). Frequency and call duration are determined by the user. The host contacts remote sites in turn to access information and to transfer event logs.

Time and Attendance. Captures hours worked by each employee for transfer to a payroll or accounting system. The feature can be programmed to:

- Generate specialized reports of time and attendance activity.
- Monitor the number of meals taken by a keyholder.
- Recognize early and late entrances and exits.
- All records can be edited and modified prior to transfer to another system.

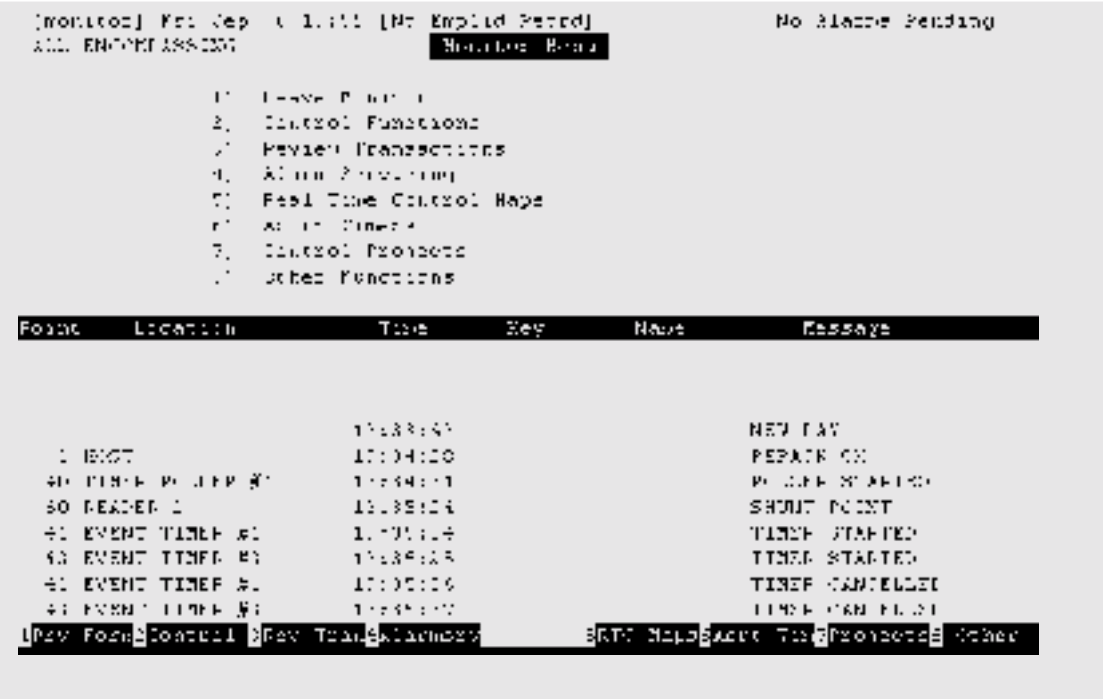
Visitor Control. Tracks visitors, prints visitor badges (black and white or color), and creates comprehensive reports of visitor activity. The feature also provides a record of who was visited and the date. It provides the company name of the visitor if applicable.

WSE ID-4000 Interface. Integrates one or more Polaroid ID-4000 photobadging systems with the SE 6000. Keyholder information and photo IDs created on the Polaroid system are transferred via a LAN or serial connection to the SE 6000. Badges can be printed on film or on PVC. Keyholder maintenance may be initiated on either system; all data is stored in a single database resident on the SE 6000.

SECTION 2
MONITOR SECURITY ACTIVITY

INTRODUCTION

System monitoring and control is performed via the monitor menu, the first selection in the system main menu. The monitor menu screen is shown below.



Notice this is a split screen, with the lower half constantly updated as transactions (any system event) occur. Most monitor screens are divided this way, and for user convenience the screen examples from this point on are shown without the transaction listings. Also, other screens not accessed from the monitor menu in this section are reduced to show the required data fields only.

SECTION ORGANIZATION

The procedures in this section are in the order shown in the monitor menu (above). The associated subscreens also follow in order (the section table of contents reflects the hierarchies).

FUNCTION KEYS

Beneath the transactions display are the applicable function keys for each screen, with the key actions shown next to the key numbers. For most function key actions, the system displays messages confirming that the action has been completed, e.g., POLLER STOPPED.

In general, F1 is used to exit from the current screen, and F7 and F8 are used respectively to display the previous screen and the next screen within the set of screens that apply to the particular data item being controlled or when there are more items then will fit into a single screen.

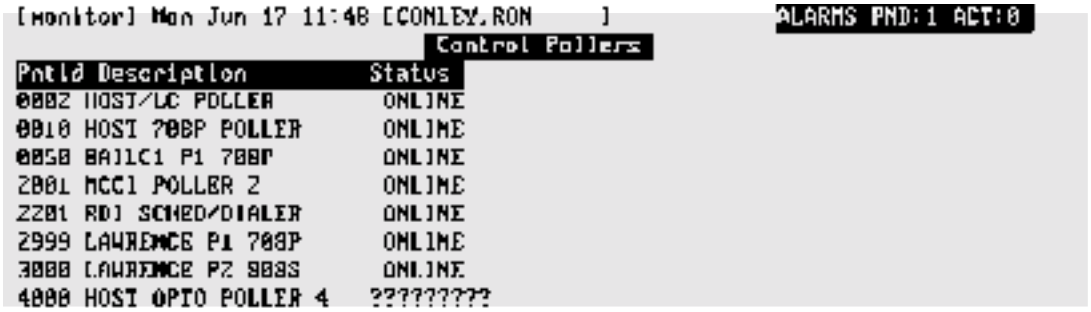
DATA ITEM SELECTION

Use the up and down arrow keys to select the data item to be controlled, then press the applicable function key for the system action to be taken.

CONTROL FUNCTIONS MENU

Pollers

The Control Pollers screen displays point ID, description, status.



Control Pollers Function Keys

F2 HALT. Stop a poller when work is to be performed on devices attached to the poller or to reload a poller parameter following a change.

F3 RESTART. Restart the poller when work is completed (system displays messages announcing each device attached to the poller as it comes back online). If there are devices with system or key checksum errors, perform a reset to the device.

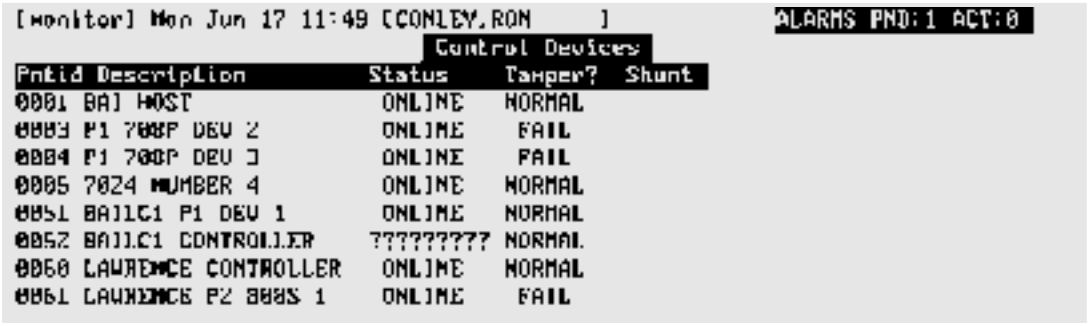
F4 DEV COMM. This function monitors communication between the pollers and the device pollers. In normal operation, the devices are asked for information by the pollers many times a second, and with a properly operating system the controller screen updates rapidly.

When F4 is pressed, a second screen displays showing the connections between the host and the devices of the particular poller selected:

Poller-device communication should be one of the first items checked whenever there is an apparent problem with the system.

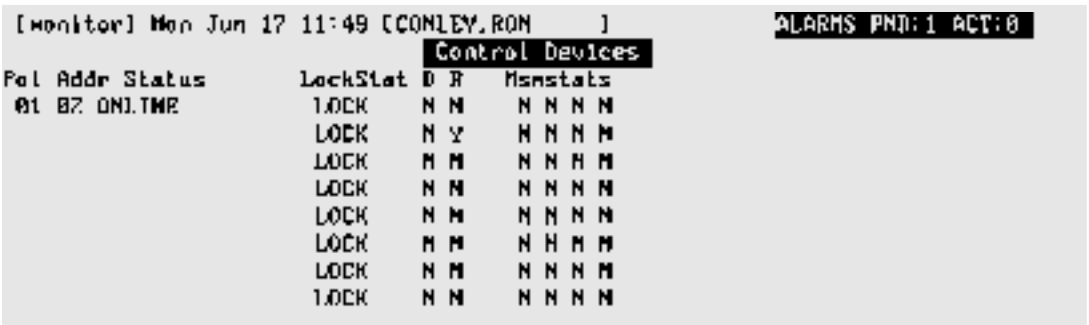
Devices

The Control Devices screen displays point ID, description, status, tamper, shunt. Applies to NexSentry, 422, and 8xx-series ACUs.



Control Devices Function Keys

F2 DEV STAT. Device Status—When F2 is pressed, a second screen displays showing the status of the particular device selected:



F3 DEV RSET. Device Reset—Used when setting up new ACUs or reestablishing repaired ACUs, or when the integrity of the data currently resident in the ACU is suspected. Downloads all host device data to the ACU and silences a latched alarm.

F4 KEY RSET. Key Reset—Used when setting up new ACUs or reestablishing repaired ACUs, or when the integrity of the data currently resident in the ACU is suspected. Downloads all host key data to the ACU.

F5 SHUNT. Shunt a device.

F6 UNSHUNT. Unshunt a device previously shunted.

Locks

The Control Locks screen displays point ID, description, lock status, shunt, sensor, coax, door status.

Control Locks Function Keys

F2 LOCK. Lock selected door. If no door is selected, F2 locks all doors in the zone.

F3 UNLOCK. Unlock selected door. If no is door selected, F3 unlocks all doors in the zone.

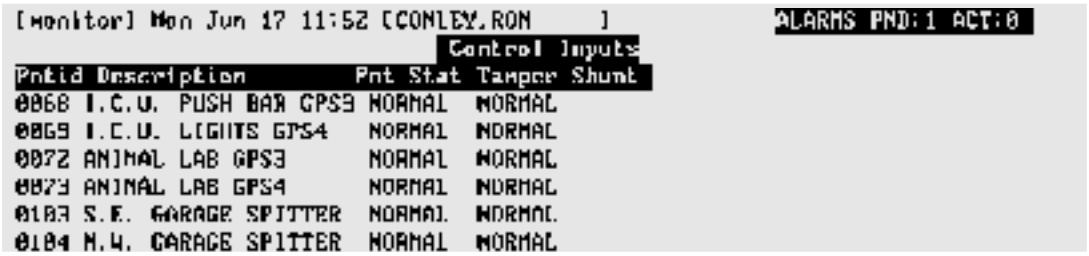
F4 TIME OPEN. Unlock selected door for the amount of time programmed at the ACU or on the reader entry screen. If no door is selected in a zone, F4 unlocks all doors in the zone for the amount of time programmed.

F5 SHUNT. Shunt a door.

F6 UNSHUNT. Unshunt a door previously shunted.

Input Points

The Control Inputs screen displays point ID, description, point status, tamper, shunt.



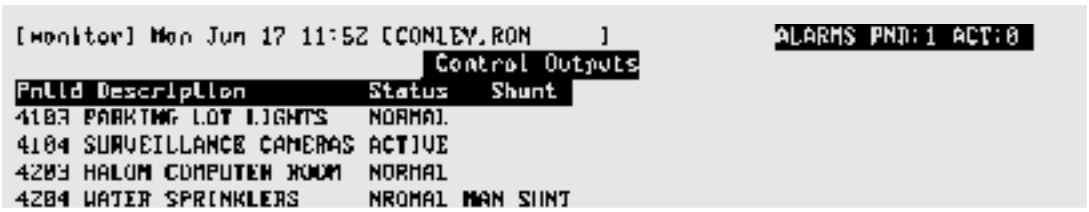
Control Inputs Function Keys

F5 SHUNT. Shunt a selected input point. If no input point is selected, F5 shunts all input points in the zone.

F6 UNSHUNT. Unshunt a selected input point previously shunted. If no input point is selected, F6 unshunts all input points in the zone.

Output Points

The Control Outputs screen displays point ID, description, status, shunt.



Control Outputs Function Keys

F2 ACTIVATE. Activate a selected output point. If no output point is selected, F2 shunts all output points in the zone.

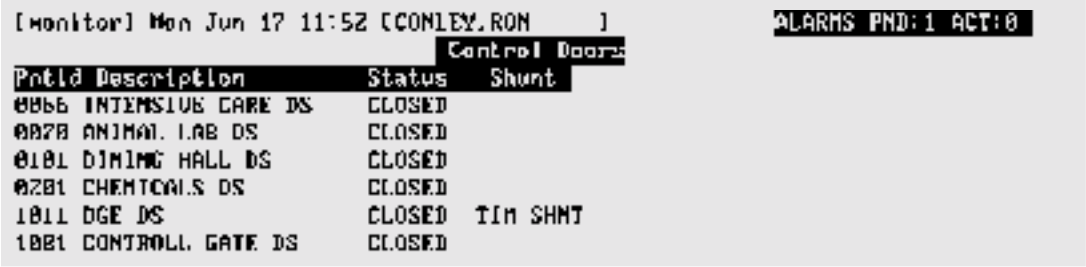
F3 NORMAL. Deactivate a selected output point. If no output point is selected, F3 deactivates all output points in the zone.

F5 SHUNT. Shunt a selected output point. If no output point is selected, F5 shunts all output points in the zone.

F6 UNSHUNT. Unshunt a selected output point previously shunted. If no output point is selected, F6 unshunts all output points in the zone.

Doors

The Control Doors screen displays point ID, description, status, and shunt of the door switches.



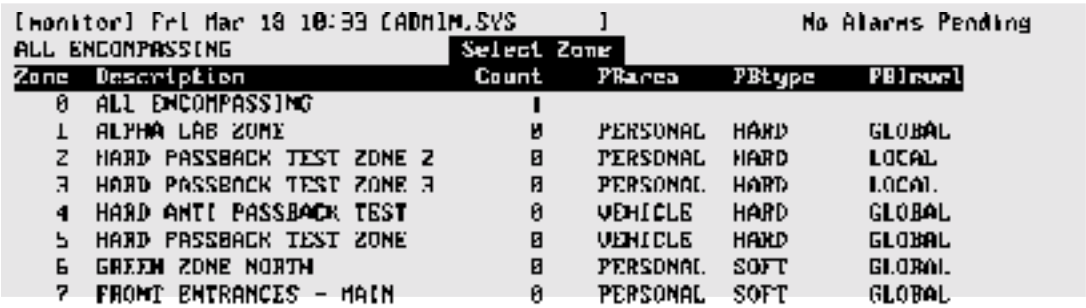
Control Doors Function Keys

F5 SHUNT. Shunt a selected door. If no door is selected, F5 shunts all doors in the zone.

F6 UNSHUNT. Unshunt a selected door previously shunted. If no door is selected, F6 unshunts all doors in the zone.

Select Zone

The Select Zone screen displays zone, description, count, PBarea, PBtype, PBlevel (see **F3 RSET CNT** below).



Use the arrow key to make the desired selection and press F2. Control activity remains exclusively for this zone until you return to the monitor menu.

The keyholder count fields apply if passback control is in effect for the zone selected

Select Zone Function Keys

F2 SEL ZONE. Select zone.

F3 RSET CNT. If passback control is in effect for a zone, the following display:

Count — Number of keyholders currently in the zone.
PBarea — Passback zone type—personal, vehicle, none.
PBtype — Passback type —hard, soft, none.
PBlevel — Passback control—global (host), local (ACU), none.

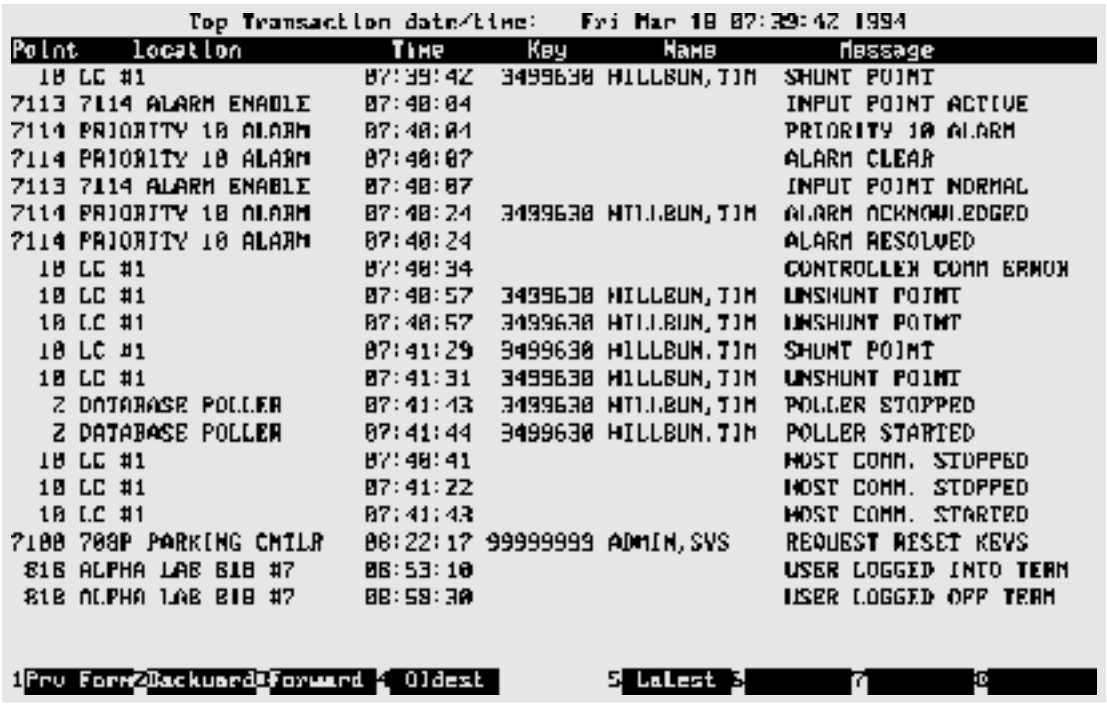
Note that zone count is automatically reset whenever a zone is selected.

Multi-user systems employ record locking techniques for keyholder file maintenance, and locked records are not updated by the passback routine that maintains keyholder location. If this occurs, the keyholder count is correct, but the passback zone report (which reads the keyholder file) does not include the locked records.

F3 corrects the zone count where privileged keyholders (not subject to passback control) have reentered a controlled zone without having exited in the normal manner or when the previous defined condition exists.

REVIEW TRANSACTIONS (FULL SCREEN)

This feature displays all transactions in the review transaction memory. Typically, the last 3,000 transactions which occurred are available. To view the screen without interruption, new transactions do not appear when using this function. If no keyboard action is taken with this feature for a five-minute period, the system returns to the monitor menu. A sample full screen follows:



Review Transactions Function Keys

F2 BACKWARD. Page backward through the transactions.

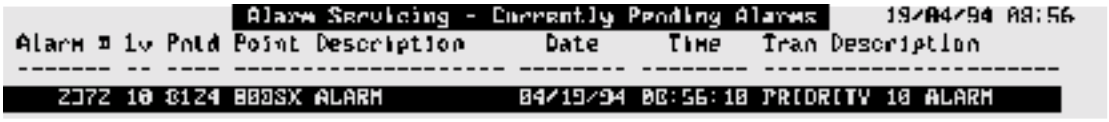
F3 FORWARD. Page forward through the transactions.

F4 OLDEST. Go to first transaction.

F5 LATEST. Go to last transaction.

ALARM SERVICING

The system emits beeps when an alarm occurs, and displays the number of pending and active alarm data in the upper-right corner of the monitor menu screen: Pending—alarm condition no longer occurring but not yet formally resolved. Active—alarm condition still occurring. Begin resolving alarms using the alarm servicing screen:



Alarm Servicing Function Keys

F2 VIEW MAP. Press F2 to display a map showing alarm location. Location indicated by the point ID in a red rectangle (other map symbols do not display when an alarm is triggered).

F3 INSTRUCT. Instructions—Press F3 to display a list of actions to take in response to the alarm.

F4 RESPONSE. Press F4 to display the alarm response entry screen. First enter Y or N in the situation resolved field (Y cannot be entered if the alarm is still occurring—take action to halt the alarm condition), then enter the actions taken. A printable record of these actions is written to disk (see *Section 3: Alarm Servicing Report*).

F5 FAST ACK. Fast Acknowledge—Press F5 and the alarm is considered resolved (use with caution because this does not allow entry of operator response to an alarm).

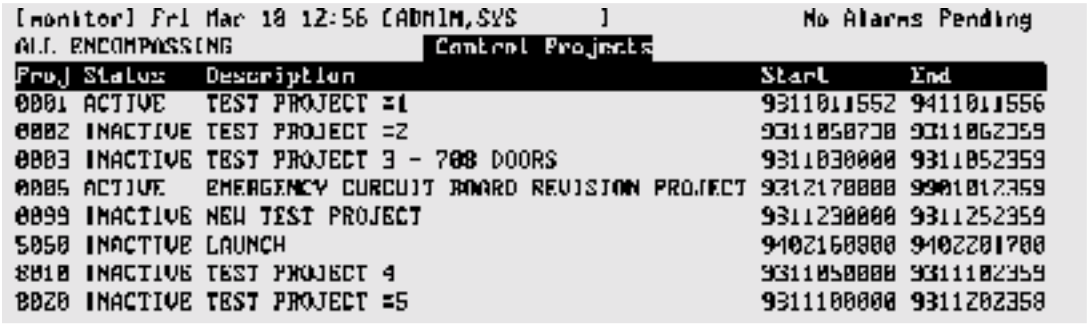
F6 SIL ALL. Silence All—Press F6 to silence beeping at all terminals.

REAL TIME CONTROL MAPS

System activity can be monitored using the system map function (created using the DRAWMAPS function—see *Section 4: Maps)*. The maps display triggered alarms (icon displays in red; goes to yellow when pending), door status (message displays), device shunt status (message displays), door unlocks (icon goes from black to white).

CONTROL PROJECTS

The Control Projects screen (not controllable on LC systems—host only) displays project, status, description, start, end. The control projects screen permits operator override of doors assigned to projects which directly affects keyholder access.



Control Projects Function Keys

F2 ACTIVATE. Activates a project.

F3 DE-ACTIV. Deactivates a project.

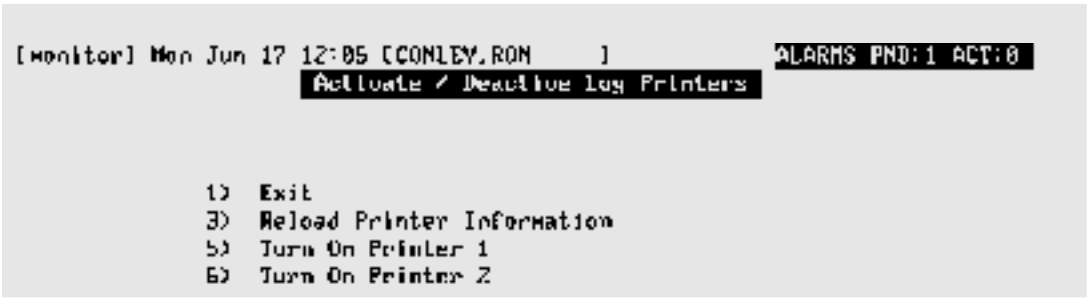
F4 NORMAL. Normalizes a project based on start/stop dates and time.

ABORT TIMERS

The Abort Timers function (F6) allows you to stop interactive timers that have started.

OTHER FUNCTIONS

Printer Control



Control Printers Function Keys

F3 RELOAD. Reloads printer data from the host which resets the printer logic and font size.

F5 PRNT ON. Switch printer #1 on or off depending on current state (used to control log printer only).
F6 PRNT ON. Switch printer #2 on or off depending on current state.

Forgive Passback

A passback violation occurs when a keyholder uses their key to reenter a door without first using their key to exit the same door. For example, a keyholder (number 1) uses their key and unlocks the door. The system flags keyholder number 1 as "in." Keyholder number 1 passes their key to keyholder number 2. When keyholder number 2 attempts to use the key, the systems gives keyholder number 1 a passback violation. This was originally developed for parking lot control. The system handles vehicle and personal passback separately.

To allow the keyholder to enter the area, use the forgive passback function.

1. Enter key number (or ALL for all keyholders); press Enter.

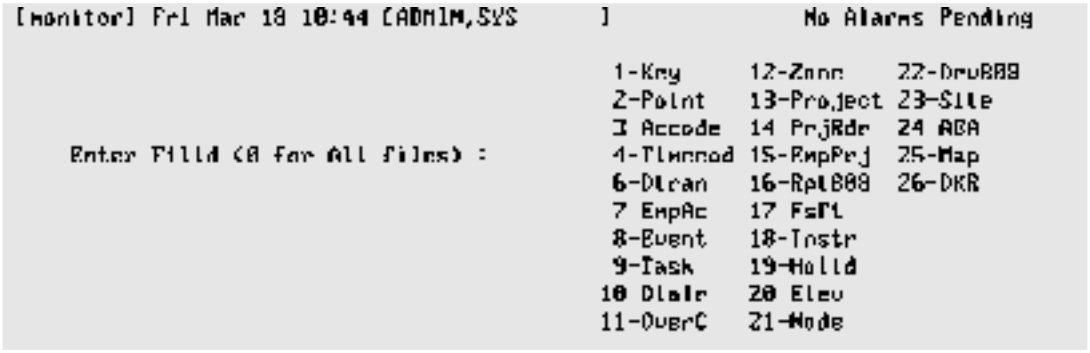
2. Press F1 to confirm the passback forgive.

Manual Access Granted

Used when a command key is not available (mislaid, stolen, etc.), this function allows the operator to grant manual access following entry of the key number (system records entry). Enter the key number and reader ID. Enter the keyholder ID if the key number is unknown. Manual access is available for all keyholders at any reader regardless of access assignments.

Force Table Download

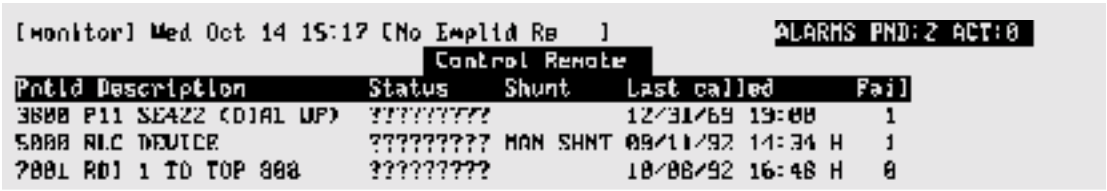
This function first writes database information to a text file, then transfers the information to host memory and LC memory (if applicable). The function is used during system servicing, and when requested by customer support. A sample screen follows:



When requested, enter the number of the table to be downloaded and press Enter. The system requests confirmation — press F1. REPACK OK displays when transfer completes.

Remote Devices

This function is used to establish a telephone connection to a remote device to perform certain actions, for example, unlock a door to a remote ATM for Service. Note that the remote device remains connected until the operator selects the device and presses F3-Hang Up.



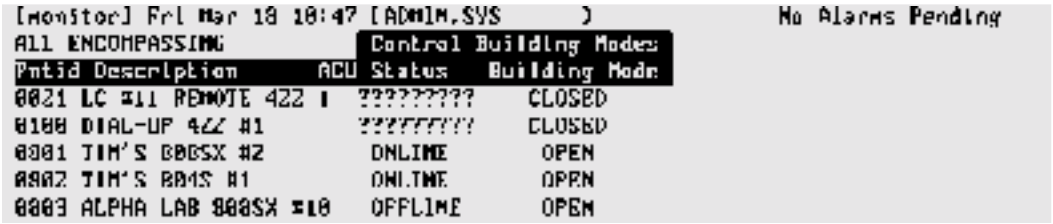
Control Remote Devices Function Keys

F2 CALL/HLD. Call device.

F3 HANGUP. Disengage connection.

Building Modes

Building modes — open, closed, limited — combined with the ACU report definitions provide an extra level of security when the building is empty or a reduced number of staff are present. Door switches and / or other monitor points active in the building open mode can be configured to generate alarms if activated when the building is in limited or closed mode. Also, if open mode, closed mode, or station readers have been defined, reader operation for those locations will change when the building mode changes. For example, an open mode reader will not read keys when the building is in limited or closed mode.



Control Building Modes Function Keys

F2 OPEN. Change current building mode to open.

F3 LIMITED. Change current building mode to limited.

F4 CLOSED. Change current building mode to closed (takes approximately one minute to complete). If a device input point configured to prevent building closure is active, the building will remain in the limited mode until the point is cleared.

Full Screen Monitoring

Displays system logs in a manner similar to the review transactions feature (see *Review Transactions—Full Screen* in this section) except that new transactions display as they occur. Use F8 to toggle between full and half screen displays.

MISCELLANEOUS INFORMATION

Disk Almost Full Warning

This feature warns operators when the disk drive has reached a specified percentage of its total capacity:

When the warning appears, take immediate action to reduce the amount of data stored on the disk (delete unwanted files, etc.).

This feature uses the DISKWARN keyword parameter located in the $DATAPATH/PARAMS.M file:

Parameter		Default Condition
DISKWARN keyword missing	—	Defaults to 90%
DISKWARN =0	—	Feature disabled
DISKWARN =***n***	—	Feature enabled; ***n*** is the range 1—99

NOTE

1. Shut down and reboot after changing DISKWARN parameters.

2. The DISK ALMOST FULL message is generated only once.

3. Since the message is generated only once, we recommend that system message #242 be changed to an alarm event by changing the alarm priority field to a value greater than 0. See *Section 6, Transactions [tranentr]* for details.

Status Screen Function Timeout

Some system functions temporarily disable the realtime display until the sub-menu is exited. The status screen function Timeout feature provides a user-defined method for controlling the length of time that the realtime display is disabled. If the system does not detect any keyboard or mouse activity for the number of seconds defined by the TIMEOUT parameter, the monitor program returns to the previous menu and resumes realtime display.

This feature uses the parameter file $DATAPATH/MONITOR, with the control parameter TIMEOUT having a numeric value in seconds:

Parameter		Default Condition
Parameter missing	—	TIMEOUT defaults to 0—feature disabled
TIMEOUT=0	—	Feature disabled
TIMEOUT=*n*	—	Feature enabled using the numeric value *n* (five digits maximum)
TIMEOUT=600	—	Feature enabled using the numeric value 600—600 seconds, default

NOTE

1. The control parameter is read by the monitor program at log-on time and remains in effect as long as the monitor program is active. A change to the Timeout value does not take effect until the user logs off, and then logs back on to the system (reboot not required).

2. This feature is operational with the following screens:

   A. The device communication function of the control pollers screen (see *Pollers* in this section).

   B. The device status function of the control devices screen (see *Devices* in this section).

Alarm Servicing — No Activity Timeout

This feature controls how long the alarm servicing screen displays when there is no keyboard or mouse activity. On Timeout, the system exits the alarm servicing program and returns to the realtime display of system events.

This feature uses the $DATAPATH/ALARMSRV parameter file, with the control parameter TIMEOUT having a numeric value in seconds: Acceptable values are:

Parameter		Default Condition
Parameter missing	—	TIMEOUT defaults to **0**—feature disabled
TIMEOUT=**0**	—	Feature disabled
TIMEOUT=***n***	—	Feature enabled using the numeric value ***n*** (five digits maximum)
TIMEOUT=**600**	—	Feature enabled using the numeric value **600**—600 seconds, default

NOTE

1. The control parameter is read by the alarm servicing program at log-on time and remains in effect as long as the alarm program is active. A change to the Timeout value does not take effect until the user logs off, and then logs back on to the system (reboots).

2. Timeout is deactivated when responding to an alarm in the alarm response screen.

Monitoring Security - Passwords

With enhanced monitor security function and the addition of password logic, any or all portions of the monitor functions can be set up to require a valid ID and password combination before the function can be initiated. In place of the factory-supplied status login, the user may create a similar login ID, with or without password, and control access to monitor capabilities. While many operators may use the generic login, individual users will have only monitor privileges consistent with their own custom security profiles.

This feature uses the PASSWORD keyword parameter located in the $DATAPATH/MONITOR file. The acceptable values are:

PASSWORD keyword missing	—	Feature disabled
PASSWORD=0	—	Feature disabled (default)
PASSWORD=1	—	Feature enabled

This feature also requires that the user has a custom security profile. See also note #1 regarding system upgrades with users created on an earlier version of the software.

Implementing the Feature

For additional information see Chapter 6, Adding a User.

1. Log on using an assigned login name and password, or use a generic login name (and optional password) as required by facility procedures.

2. With the password feature enabled, any action attempted from the monitor for which permission has not been granted causes the system to prompt for a login name and password.

3. If the login name and password entered are valid, the associated security profile initiates the action requested (see note #4).

4. If the feature is disabled or an incorrect login / password is entered, the system displays PERMISSION DENIED.

NOTE

1. If your system has been upgraded, and users created on a previous release have been saved, their user profiles must be updated with the new monitor security privileges. To do this, log on as addusers with the correct password, select system administration, and then select add users. Update the security profile for each user as follows:

   - Enter the user ID
   - Select modify—F5
   - Press the return key through all fields
   - Store the updated profile—F8

   Repeat for all applicable users. The new custom security information is appended without changing the current privileges.

2. If the password keyword parameter is changed, users must log off then log back on (reboot) before a change is recognized by the monitor program.

3. All functions that generate log messages are logged with the user ID entered to gain access to the requested function.

4. Permissions associated with the entered login ID remain in effect until the operator returns to the point where the login ID and password were required, or, if the status screen function Timeout feature has been enabled, the screen itself will Timeout (see *Status Screen Function Timeout Feature* in this section).

Modified Usage of Invalid Facility Code Log

This feature suppresses a keyholder's name from the monitoring screen and various reports when an INVALID FACILITY CODE message is logged. In some cases, this resulted in a log message erroneously associating a valid keyholder with an invalid facility. This function is automatic and does not require operator action.

NOTE

This occurred with the 708 type device where different facility codes were used on different buildings. It only applies to 1030/1040 cards with facility codes where a user has keys with multiple codes.

1. This feature affects the following displays and reports:

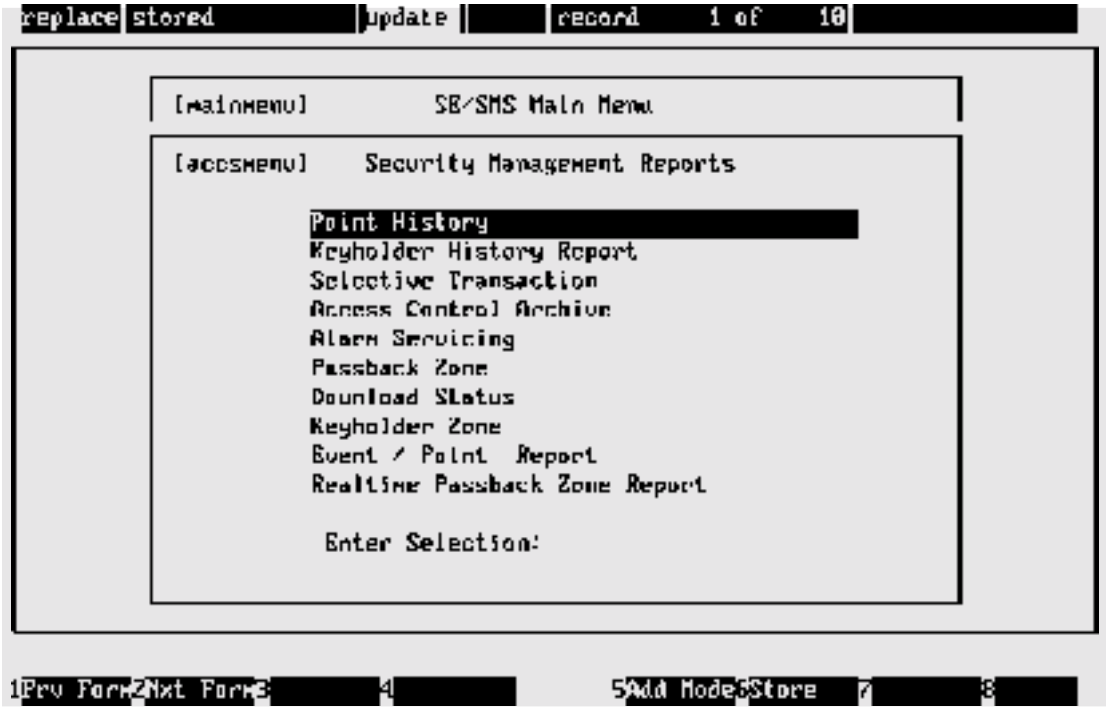
   - Monitor screen, both full- and half-screen displays
   - Review transactions screen
   - Point history report
   - Keyholder history report
   - Transaction history report - all sort options
   - Archive history report - all sort options

2. Log records are not altered.

SECTION 3
SECURITY REPORTS

INTRODUCTION

Security management reports provide a permanent record of transactions, and are also used to examine specific events. The reports are accessed through the security management reports menu screen, [accsmenu], via the main menu. In this section, the reports are documented following the security management reports menu sequence (see section table of contents). A sample [accsmenu] screen follows:



All screens in this section show the system default values, with most screen fields requiring a numeric range entry. For example, the default range for keyholders is 1 — 999999999 (to reduce waiting time while a report is generating, enter the smallest range of numbers for each category which will still provide the information required). Other screen fields include choices for a specific data item, date ranges, regular or extended information, and report sequencing. When all fields have been entered, press Enter (Yes - default) to begin report generation:

Once compiled, a report output selection displays. Normally, 1 (system report printer) or D (display at terminal) is chosen. Report totals are printed at the end of each report.

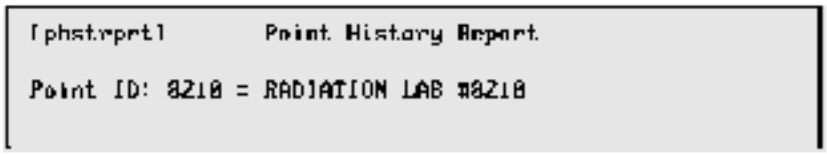
NOTE

1. Some reports are over-wide (132 characters instead of the standard 80 characters), and have been formatted to use a smaller print size not available with some terminals (HP printers can handle the smaller print). These reports can be displayed but will 'wrap'; that is, some lines continue to the next display line . In such a case, use the display option to check report details, then use one of the print options to create a hard copy of the report.

2. For color PCs with Reflections 4 software, or an HP700/44, the display automatically changes to the 132-column mode for any reports with lines exceeding 80 characters.

POINT HISTORY REPORT

The point history report, [phstrprt], lists transaction activity at a specific point. The report lists the key number and name (if any) associated with a transaction, date and time, and description. To facilitate processing, only the last 20 transactions are used. If more than the last 20 transactions are required, use the transaction history report. A sample [phstrprt] screen follows:

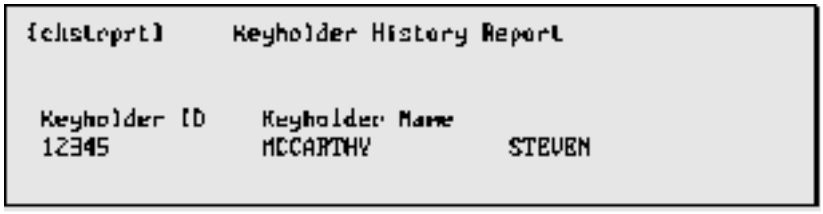


Point History — Sample Report

```
06/27/96                          Packlett Industries                          PAGE    1
14:36                             Point History

    KeyhldID   Keyholder Name                    Date       Time       Access Description
    ________   _________________                 _____      ____       ___________________

      166603   HALSTON RICHARD                   06/24/96   16:50:47   MANUAL LOCK
      166603   HALSTON RICHARD                   06/24/96   16:50:46   MANUAL OPEN
      166755   GREENE LORRAINE                   06/24/96   16:50:45   MANUAL LOCK
      166755   GREENE LORRAINE                   06/24/96   16:50:44   MANUAL OPEN
      161221   ROBINS JAMES                      06/24/96   16:50:43   MANUAL LOCK
      161221   ROBINS JAMES                      06/24/96   16:50:42   MANUAL OPEN
      163878   COUSINS TERRY                     06/24/96   15:09:23   MANUAL LOCK
      163878   COUSINS TERRY                     06/24/96   15:09:21   MANUAL OPEN
      165446   AVERY JOE                         06/21/96   14:19:22   UNABLE TO UNLOCK DOOR
      165446   AVERY JOE                         06/21/96   13:55:47   UNABLE TO LOCK DOOR
```

KEYHOLDER HISTORY REPORT

The keyholder history report, [chstrprt], lists activities for a specific keyholder. Also, the report can be used for tracking actions taken by a system operator. The report contains point or sensor data showing where activity occurred, date and time, and description. To facilitate processing, only the last 20 transactions are used. If more than the last 20 transactions are required, use the transaction history report. A sample [chstrprt] screen follows:

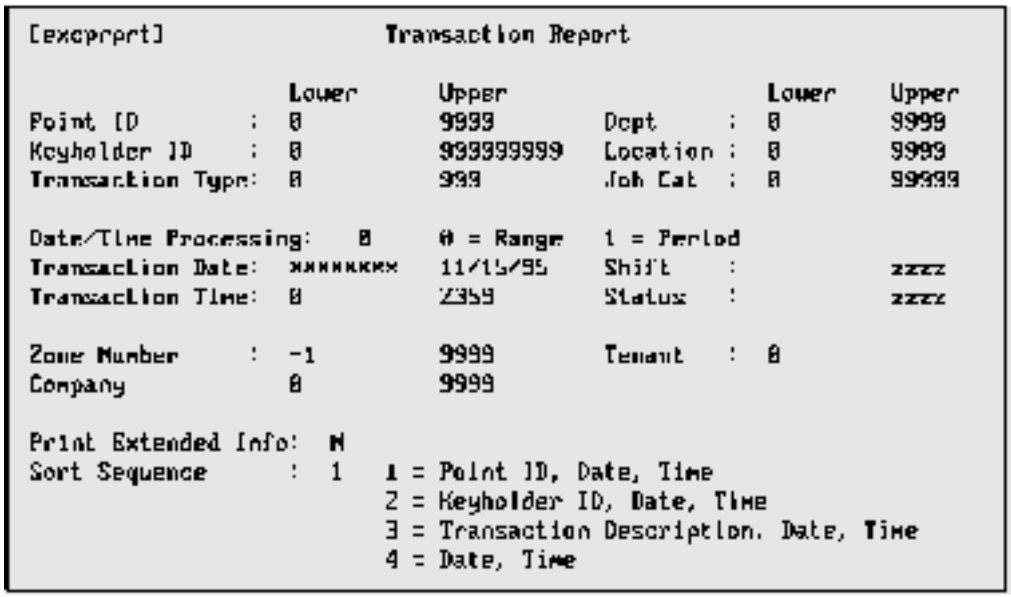


Keyholder History — Sample Report

```
06/27/96                          Packlett Industries                          PAGE    1
14:36                             Point History

  Point  Point Description                Date            Time          Access Type
  _____  _____________________             ________        ________      ____________________

Keyholder      2771  Dale, Deborah

   0225  RDI-8082-SEN2                     06/27/96        09:32:52      ACCESS GRANTED
   0221  RDI-8082-SEN1                     06/27/96        07:34:24      ACCESS GRANTED
   0215  RDI-8081-SEN1-READER              06/27/96        07:34:22      ACCESS GRANTED
   0220  T&A READER 3 N/A                  06/26/96        15:40:42      MANUAL OPEN
   0210  T&A READER 2 OUT                  06/26/96        15:40:40      MANUAL OPEN
   0200  T&A READER 1 IN                   06/26/96        15:40:34      MANUAL OPEN
   0120  ELEVATOR FREIGHT CAR              06/26/96        15:40:31      MANUAL LOCK
```

TRANSACTION HISTORY REPORT

The transaction history report, [excprprt], lists all transactions according to selected criteria. The transaction report function is used to create a who, what, where, and when report of all transactions. This function includes information about the ID and description of the point or sensor where the transaction occurred, the zone number of the point or sensor, the date and time of the transaction, the type of access (for an access transaction) and the ID and name of the keyholder involved with the transaction, if any. Two report types are available: short and extended. The short report accesses all standard information; the extended report does the same but includes user-defined field information. A sample [excprprt] screen follows:



```
[excprprt]                Transaction Report

                    Lower      Upper                    Lower    Upper
Point ID        :   0          9999        Dept     :   0        9999
Keyholder ID    :   0          999999999   Location :   0        9999
Transaction Type:   0          999         Job Cat  :   0        99999

Date/Time Processing:    0     0 = Range   1 = Period
Transaction Date:   xxxxxxxx   11/15/95    Shift    :            zzzz
Transaction Time:   0          2359        Status   :            zzzz

Zone Number     :   -1         9999        Tenant   :   0
Company             0          9999

Print Extended Info:  N
Sort Sequence       :  1   1 = Point ID, Date, Time
                           2 = Keyholder ID, Date, Time
                           3 = Transaction Description, Date, Time
                           4 = Date, Time
```

Transaction History — Sample Report

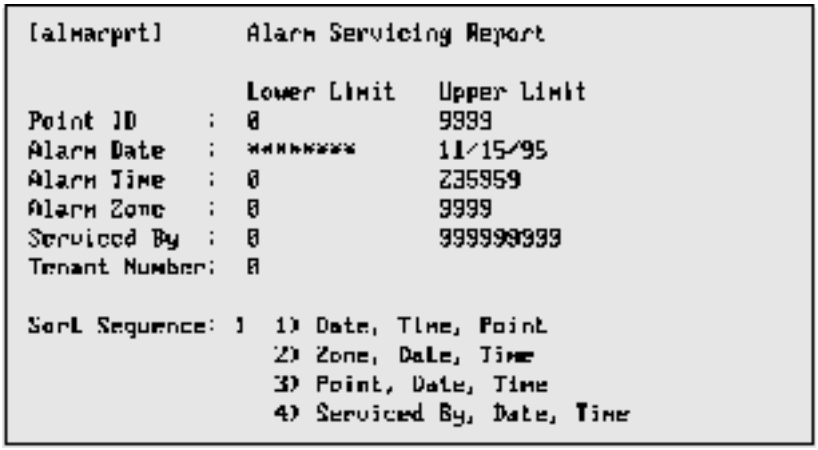
```
11/15/96                                  SHARPSMITH LABS, INC.                    Page 1
10:34                                     Access Control Transaction Report

Point  Point Description       Zone  Date     Time     Access Type              Keyholder  Keyholder Name    Key No
_____  ______________________  ____  _____    _____    ________________________ _________  ________________  ______

   1   HOST                    801  10/28/96 11:12:00 FORGIVE PASSBACK           661094  Stanling, Bob     34421
   1   HOST                      0  10/28/96 11:23:00 REPACK OK
   1   HOST                    801  10/28/96 13:37:00 FORGIVE PASSBACK           662886  Jonesman, Linda   32211
   1   HOST                    001  10/28/96 14:12:00 FORGIVE PASSBACK           656633  Buchmann, G.T.    34588
   1   HOST                      0  10/28/96 14:17:00 REPACK OK
   1   HOST                      0  10/28/96 14:49:00 FORGIVE PASSBACK           641918  Saunder, Rick     34876
```

ACCESS CONTROL ARCHIVE REPORT

The access control archive report, [acrtrprt], is identical to the transaction history report (previous report) except that it reads data from an archive tape rather than from the system database.

ALARM SERVICING REPORT

The alarm servicing report, [almarprt], details actions taken by operators in response to alarms. A sample [almarprt] screen follows:

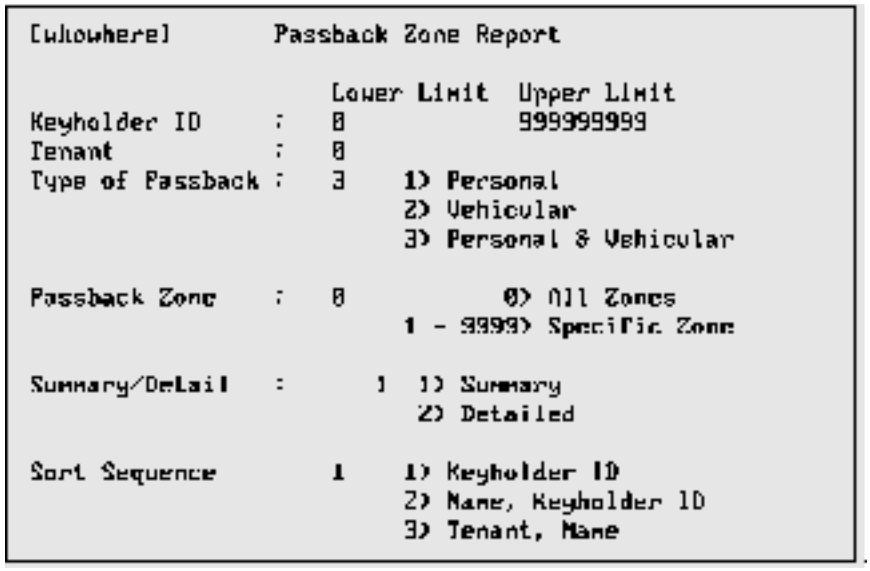


Alarm Servicing — Sample Report

```
06/27/96                                    PacAtlantic Racing                              PAGE  1
15:01                                       Alarm Master List

Alarm No  Alrmtime  Alrmdate  Point Zone  Resp Time  Resp Date  Clear Time  Clear Date  Serviced By
________  ________  ________  _____ ____  _________  _________  __________  __________  ___________

Point Descrip = CHEMICALS GPS 3
   2851  09:18:00  06/26/96     20    3  14:19:05   06/26/96   11:10:10    06/26/96    Maintenance

Operator Response:                          Alarm Instructions:

CALLED FIRE DEPT.                           PUT  ON MASK
CLEARED BUILDING                            CALL FIRE DEPARTMENT IMMEDIATELY
OPENED VENTS                                EVACUATE ALL PEOPLE FROM BUILDING
LEFT BUILDING                               OPEN  EMERGENCY VENTS
REENTERED WHEN ALL CLEAR                    LEAVE BUILDING
```

PASSBACK ZONE REPORT

The passback zone report, [whowhere], lists keyholders currently present in passback zones. The summary selection provides totals by zone, while the detailed report lists specific keyholders. The source for the information is the keyholder file. A sample [whowhere] screen follows:

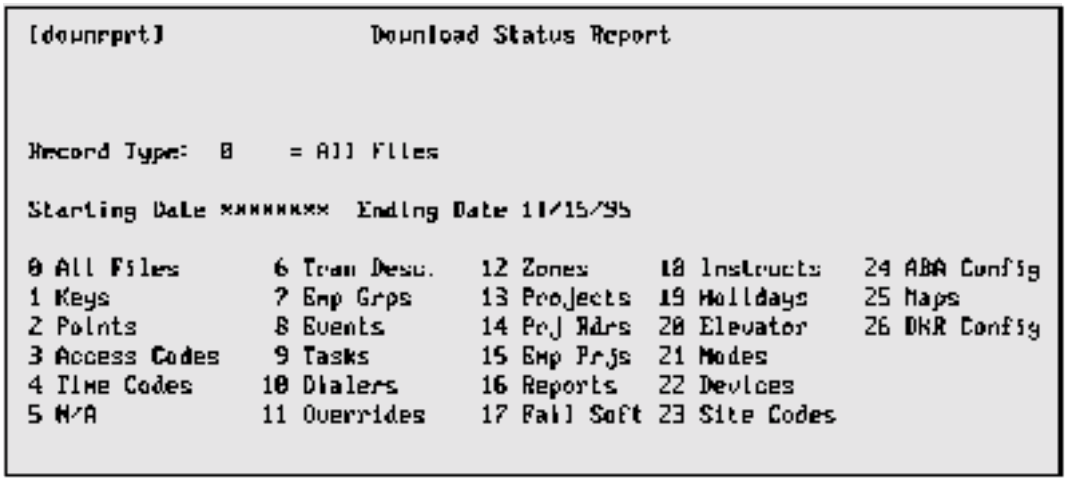


Passback Zone — Sample Report

```
04/05/96                Easthaven Manufacturing             Page  1
14:43                   Passback Zone Report

Keyholder    Key No  Keyholder Name               Tenant   Pzone   Vzone
_________    ______  ___________________________ _______  ______  ______

  1055699    83383   MAITLING, JACK                  0      -1      -1
  1061128    84128   LYONS, CINDY                    0      -1      -1
  1086201    83361   DENEUVE, DENISE                 0       0      -1
  1099004    86660   SMITH, PAULA                    0       1       2
  1100015    87083   MACKLING, JACKIE                0      -1      -1
  1116345    88883   FLYNN, SEAN                     0      -1      -1
```

DOWNLOAD STATUS REPORT

The download status report, [downrprt], is used to create an audit-trail of system information change attempts, the devices affected, who attempted the changes, and when and if the changes were successful. A sample screen follows:



Download Status — Sample Report

```
06/27/96                                  Nevadia Industries                PAGE  1
15:03                                     Download Status Report

 Serial #  Key Value  File  Descrip Typ  Date      Time   Maint By  Status              Point  Point  Descrip
 --------  ---------  ----  ------- ---  --------  -----  --------  ------              -----  ---------------

    21729         76     2  Points  Chg  06/27/96  08:34  Paul      Received & Processed    0  HOST
    21730         76     2  Points  Chg  06/27/96  08:34  Paul      Received & Processed   60  1ST CNTRLLER
    21731         76     2  Points  Chg  06/27/96  08:34  Paul      Received & Processed   61  CNTRL P28081
    21723      21463     8  Events  Del  06/27/96  08:31  Paul      Received & Processed    0  HOST
    21724      21463     8  Events  Del  06/27/96  08:31  Paul      Received & Processed   52  BAIL C1 CNTRL
    21725      21463     8  Events  Del  06/27/96  08:31  Paul      Received & Processed   60  1ST CNTRLLER
    21726      21463     8  Events  Del  06/27/96  08:31  Paul      Received & Processed   61  CNTRL  P28081
```

Possible system messages for this report are:

Unprocessed — Information changed in the database, but has not yet been sent to the communications program module.

Before Transmit — Information has been sent to the communications program module, but has not yet been sent to target device.

Transmitted — Data has been sent from the host to the target device, but acknowledgment has not yet been received from the target device.

Received and Processed — Information successfully transmitted by the host and successfully received by the target device (download completed).

ERR Transmitting Data — Error on host side of transmission. Normally, this means that the host communications program module was unable to complete the requested download.

ERR Receiving Data — Information successfully transmitted by the host, but the target device was unable to receive.

KEYHOLDER ZONE REPORT

The report lists the most recent zone information for all keyholders that meet the search criteria; however, information is not necessarily current. A sample [kyznrprt] screen follows:

```
[kyznrprt]      Keyholder Zone Report

                     Lower Limit  Upper Limit
Keyholder ID     :   0            999999999
Tenant           :   0

Find By          :   1     1) Zone
                           2) Area
Zone Number      :   0           0) All Zones
                         1 - 9999) Specific Zone
Area Number      :   0

Summary/Detail   :       1  1) Summary
                            2) Detailed

Sort Sequence        1      1) Keyholder ID
                            2) Keyholder Name Keyholder ID
                            3) Zone, Keyholder Name
```

Keyholder Zone — Sample Report

```
05/12/96                          Vogler Vineyards                          Page   1
14:41                             Keyholder Zone Report

   Keyholder  Keyholder Name       Tenant  Point  Point Description  Date      Time      Zone
   _________  ___________________  ______  _____  _________________  ________  ________  ____

       10556  MAITLING JAMES       0       3120   808SX RDR 2        04/02/96 16:48:12    0
       10564  LYONS SHELLEY        0       3120   808SX RDR 2        04/02/96 16:48:12    0
       10569  MCDUFF GORDON        0       3120   808SX RDR 2        04/02/96 16:48:12    0
       10622  DENEUVE DENISE       0       3120   808SX RDR 2        04/02/96 16:48:12    0
       10643  SMITH PAULA          0       3120   808SX RDR 2        04/02/96 16:48:12    0
       10701  HERALD RICHARD       0       3120   808SX RDR 2        04/02/96 16:48:12    0
```

EVENT / POINT REPORT

The event / point report, [evptrprt], lists the number of events of a particular type that have occurred at a point or within a range of points. The report is limited to the current contents of the archive history file. A sample [evptrprt] screen follows:

```
[evptrprt]              Event / Point Report


                    Lower       Upper
Point ID        :   0           9999
Transaction Type:   0           999

Date/Time Processing:   0       0 - Range   1 - Period

Transaction Date:   ********    11/15/95
Transaction Time:   0           235959

Zone Number     :   -1          9999

Sort Sequence   :   1   1 = Point ID
                        2 = Transaction Type
```

Event / Point — Sample Report

```
03/17/96                        Security Electronics          Page  1
09:15                           Event/Point Report

Point  Point Description        Tran.   Tran. Description         Occurrences
_____________________________________________________________    ___________


    1  HOST                      231    PROJECT DEACTIVATED                2
    1  HOST                      242    DISK ALMOST FULL                   5
    2  DATA BASE POLLER           24    POLLER STARTED                     1
    2  DATA BASE POLLER           25    POLLER STOPPED                     1
    4  808/422 POLLER            222    POLLER STOPPED                     2
    4  808/422 POLLER            224    POLLER STARTED                    12
```

REALTIME PASSBACK ZONE REPORT

The realtime passback zone report, [rpasrprt], is essentially the same report as the passback zone report (described earlier in this section), with one important difference. The realtime report is created directly from shared memory instead of from the database. This feature substantially reduces the amount of time necessary to find out where keyholders are currently located. This can be very useful for monitoring hazardous areas, or when it is important to rapidly determine the number or identity of the keyholders in a particular zone.

```
[rpasrpct]   Realtime Passback Zone Report

                      Lower Limit  Upper Limit
Keyholder ID      :   0            999999999
Tenant            :   0
Type of Passback  :   3    1) Personal
                           2) Vehicular
                           3) Personal & Vehicular

Passback Zone     :   0          0) All Zones
                           1 - 9999) Specific Zone

Summary/Detail    :       1  1) Summary
                             2) Detailed

Sort Sequence         1    1) Keyholder ID
                           2) Name, Keyholder ID
                           3) Tenant, Name
```

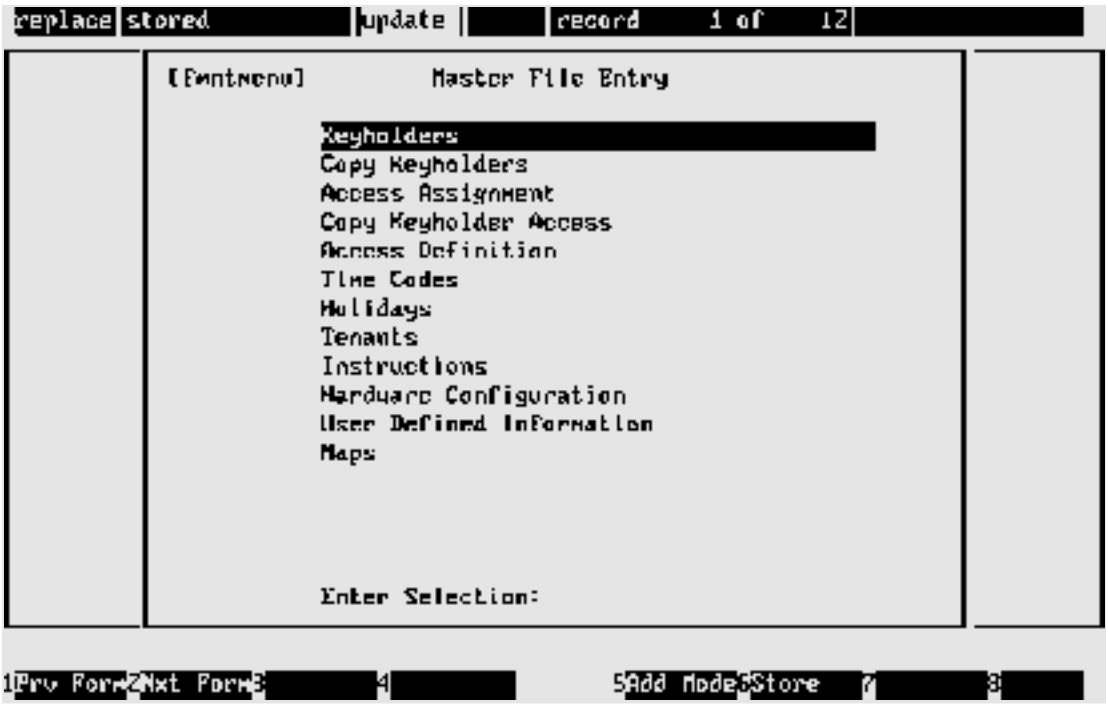
REALTIME PASSBACK DETAIL — SAMPLE REPORT

```
03/14/96                    McPowell-Angus Aviation              Page 1
15:18                       Realtime Passback Detail Report

 Keyholder   Key No  Keyholder Name                 Tenant  Pzone  Vzone
 _________ ________  ___________________________    _______ _____  _____
    223141   188954  McDaniels, Jeff                   0     -1     -1
    237473   140226  Wellington, Lambert               0     -1     -1
    233974   195226  Du Pont, Michael                  0     -1     -1
    239965   200026  Senter, Carol                     0     -1     -1
    248366   180463  Pons, Antonia                     0     -1   7100
    249037   143511  Segwick, G.J.                     0     -1     -1
```

SECTION 4
MASTER FILE ENTRY

INTRODUCTION

The master file entry procedures are used to create and maintain the database. All initial system data is entered following the methods detailed in this section. The data item menu screens are accessed via the master file entry menu [fmntmenu], displayed via the main menu. A sample [fmntmenu] screen follows.



Some master file entry procedures are used more frequently than others. For example, keyholder data is usually added, changed, and deleted daily. On the other hand, additions or changes to system configuration information may occur only once every several months.

Screen Access

The procedures in this section are in the order as they appear on the [fmntmenu] screen (above). Following each menu entry are the associated subscreens, again in order (the section table of contents reflects the hierarchy). After the current screen has been saved (F6), most subscreens display by pressing F2 but some display automatically.

KEYHOLDERS

Four data entry screens are used to add new keyholders to the system, and to change or delete existing keyholder information:

1. Keyholder Entry - Page 1, [key_entr]. Used to enter primary keyholder information.
2. Keyholder Entry - Page 2, [key1entr]. Used to enter optional keyholder information.
3. Keyholder Access Entry, [empgentr]. Used to enter access codes, access groups (keyholder access assignments), etc.
4. Project Assignment [epj_entr]. Used to enter projects, if applicable.

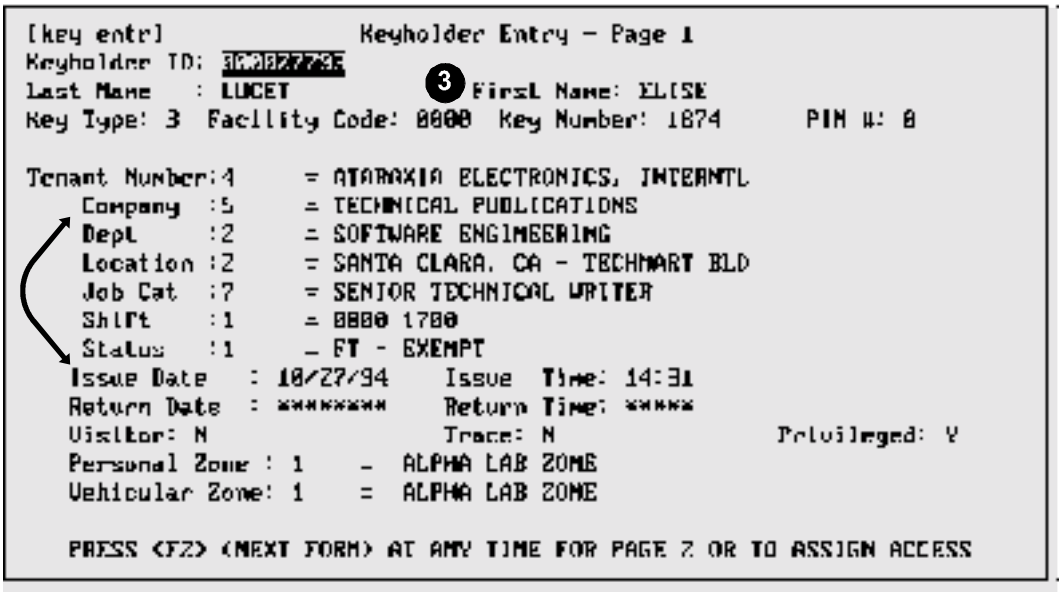
The first screen, [key_entr], is accessed from Keyholders (first item in the [fmntmenu] menu); the other screens are displayed using F2 after the previous screen has been saved.

IMPORTANT

1. All keyholder data is linked to the keyholder ID rather than by key number or name. This allows the change or removal of key numbers from the system—a frequent requirement—without affecting entire keyholder records.

2. For future reporting purposes, we recommend that the keyholder ID record be retained when a keyholder leaves your facility. To block the keyholder ID from normal system processing, enter zero for the key number in [key_entr], and/or delete access assignments (Esc, d, r) in [empgentr].

Keyholder Entry—Page 1 [key_entr]



Keyholder ID. Required in the Add mode (the system denies further screen access until this field is entered). Enter a unique nine-digit maximum keyholder ID number (alphabetical letters are not supported).

Last Name. Optional. Enter the keyholder's last name.

3 **First Name**. Optional. Enter the keyholder's first name.

NOTE

Names are index-maintained rather than sequential, allowing quick keyholder record search by name or partial name.

Key Type. Required. Enter the key type code number:

* = No key (default)
1 = 1030
2 = 1040
3 = 1050
4 = 1060 and digital keys

Note that if the key type is unknown, use type 3. This can be changed later if necessary.

Facility code. Required for 1030 / 1040 key types. Enter the four-digit facility code printed on 1030 and 1040 keys; example: DO34. Default is **** — No facility code.

Key Number. Conditional. Enter an eight-digit maximum key number. If you do not wish to select a key number at this point, the system default 0 is entered automatically.

PIN # (personal identification number). Required if certain keypad identification equipment is used with your system (MCCI or VIP-2 poller); otherwise, disregard this field.

Tenant Number. Optional. Enter a four-digit maximum tenant code (*zoom* available). Default is tenant 0.

User-defined field titles. Using the control file maintenance screen (see *Control File Maintenance [ctrlentr]* in Section 6), these field titles can be changed to suit the individual user. Entries are numeric and point to a description table. (Applies also to fields *usr1* through *usr6*, and *Remarks*, in [key1entr].)

Company — Keyholder's company name
Dept — Keyholder's department name
Location — Location of keyholder's department
Jobcat — Keyholder's job category
Shift — Keyholder's normal working hours
Emp Stat — Keyholder's status

Issue Date. Optional. Enter the date that the access control card for the keyholder will become valid. Default is current system date. Note that a future date will not permit access until that date is reached.

Issue Time. Optional. Enter the time that the access control card for the keyholder will become valid. Note that this only applies with host access. Default is current system time.

Return Date. Optional—Recommended if keyholder is a visitor (see *Visitor* below). Enter the final date that the keyholder's card will be valid. Default is ******** — No expiration date.

Return Time. Optional—Recommended if keyholder is a visitor (see *Visitor* below). Enter the time on the final date that the keyholder's card will be valid. Default is *blank*—No expiration time. Note that this only applies with host access.

Visitor. Recommended. A Y/N field indicating if the keyholder is a visitor. If Y, it is advisable to enter a return date and time (previous fields). Note that this is listed for reference only. Default is N.

Trace. Optional. A Y/N field indicating if the keyholder is to be monitored (movements traced while in the building). Trace monitors doors, readers, and records. Using Trace causes an extra key trace log message. This feature is sometimes desirable if the keyholder is a visitor (see previous field). Default is N.

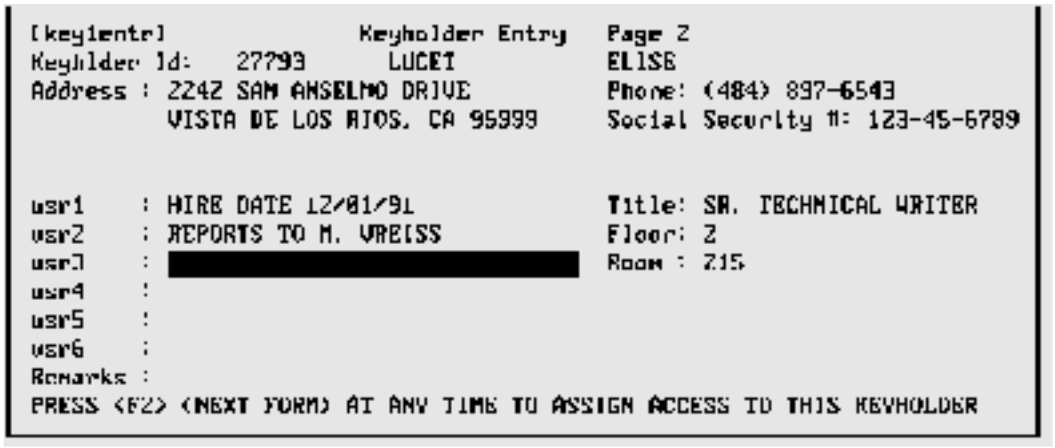
Privileged. Conditional. A Y / N field for ACUs supporting building modes and global anti-passback. Enter Y if this keyholder can change building modes at a remote reader and is immune from anti-passback. Default is N.

Personal Zone. If passback is in effect, the zone where the keyholder is currently located and reported to the system by the reader last used by the keyholder. When setting up the database, use the default (-1, unknown).

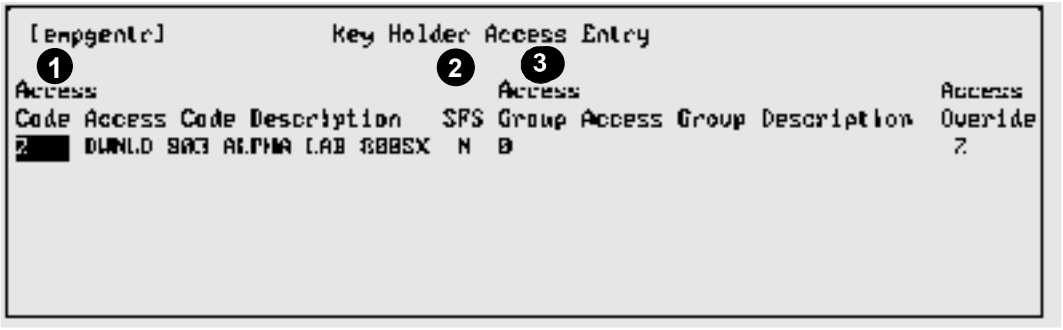
Vehicular Zone. The zone (car park) where the keyholder's vehicle is currently located; reported to the system by the parking lot reader last used by the keyholder. When setting up the database, use the default (-1, unknown).

Keyholder Entry—Page 2 [key1entr]

The data entered in this screen is for information only. Field entry is self-evident (field titles *usr1* through *usr6*, and *Remarks*, can be changed to suit the individual user (see *Section 6: System Administration*). Note that data is unique and not selected as table reference (see user-defined field titles, reference 9). Simply complete those fields required by your company, store (F6), then press F2 to display the access assignment screen [empgentr].



Keyholder Access Entry [empgentr]



Access Code. Optional. Enter an access code number that applies to this keyholder (the system automatically enters the access code description). Default is 0—No access code.

NOTE

There is no limit to the number of access codes that can be assigned, with the following two exceptions:

1. Do not assign a keyholder more than one access code for a single NexSentry, 8xx series, or 422 ACU.

2. The system will not allow you to combine two access codes with the same download device ID number in one access group.

3. Do not assign two access groups with codes for the same download device ID.

SFS (smart failsoft option). Optional. Smart failsoft access codes are used when communications between the host and ACU are disrupted for more than 15 seconds. Enter

Y if the downloaded access code is to be sent to the ACU as a smart failsoft access code. Default is N. Note that this is used only in conjunction with the host access codes.

NOTE

The smart failsoft option is not supported with any keys used in conjunction with 708P and 718P ACUs, but a function is built in to the units which does provide some measure of failsoft protection in the event of a communications failure with the host.

The 708P and 718P ACUs can be programmed to accept up to 25 command keys, and access is allowed when these are presented (eight doors maximum). Usually, the command keys selected are those issued to managerial and engineering staff, and to persons responsible for building maintenance.

This feature is limited to some extent in that time codes cannot be used in conjunction with this special programming, and event entries (door opening records, in this case) are not logged.

3 **Access Group**. Optional. Enter an access group number (no limit) that applies to this keyholder (the system automatically enters the access group description). Default is 0—No access group.

Note

There is no limit to the number of access codes that can be assigned, with the following two exceptions:

1. Do not assign a keyholder more than one access code for a single NexSentry, 8xx series, or 422 series ACU.

2. The system will not allow you to combine two access codes with the same download device ID number in one access group.

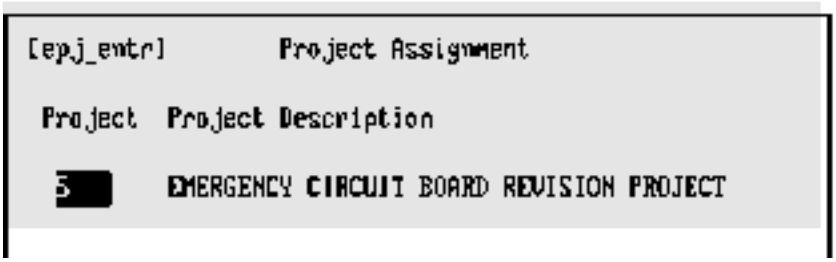
3. Do not assign two access groups with codes for the same download devices.

4 **Access Override**. Optional (*zoom* available). Enter the access override code that applies to this keyholder. Default is 0—No access override code.

Project Assignment [epj_entr]

If the keyholder has been assigned to a project, enter the project number using the [epj_entr] screen (multiple projects can be assigned). Display this screen by pressing F2 after the access assignment screen (previous screen) has been saved (F6). Note that the project function will not work properly unless the host provides access control.

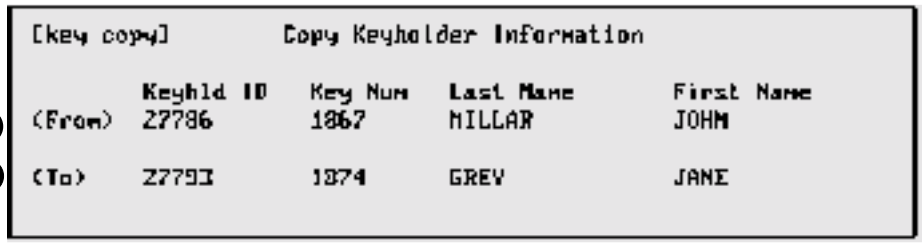
A sample [epj_entr] screen follows. Enter the project number (*zoom* available) then press Enter; the project description displays automatically. If multiple projects are to be assigned, enter and store each one separately.



COPY KEYHOLDERS

Copy Keyholder Information

Used when creating new keyholders who share data with existing keyholders, the [key_copy] screen is an important timesaving feature. A sample screen follows:



From. Enter an existing keyholder ID (*zoom* available). The system automatically supplies the key number and the keyholder names.

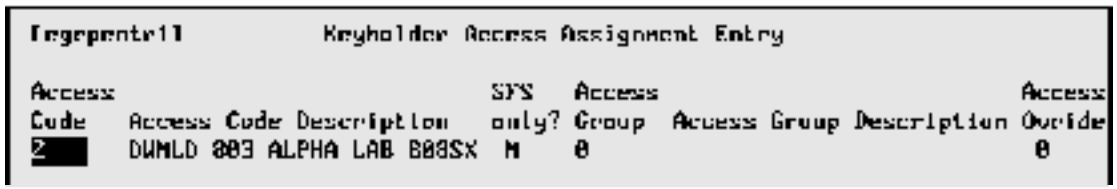
To. Enter the new keyholder ID, new key number and new keyholder name.

System responds with Okay to continue? When complete. Enter Y and a new keyholder record for the To keyholder is automatically created, with identical parameters as the From keyholder. Changes and corrections for the new ID are made as required using the various keyholder data entry screens.

ACCESS ASSIGNMENT

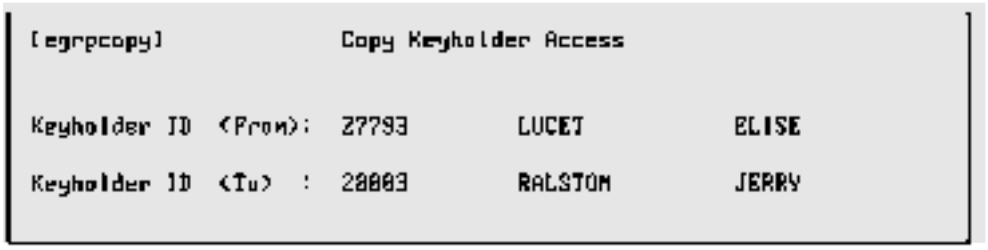
Keyholder Access Assignment [egrpentr]

The [egrpentr] and [egrpentr1] screens, accessed from *Access Assignment* (third item in the [fmntmenu] menu), are used as a fast way to make access assignments without using the keyholder data entry screens. Data entry is the same as for the keyholder access entry screen [empgentr]. The keyholder access allows only assignment permissions without access to keyholder screen. A sample screen showing [egrpentr] and [egrpentr1] follows:



COPY KEYHOLDER ACCESS [ergcopy]

The copy keyholder access screen, [egrpcopy], is used in the same way as the copy keyholder information screen for copying keyholders with similar access assignments. This is especially useful where multiple codes/groups are assigned on keys.



ACCESS DEFINITION

The access definition selection in the master file entry menu displays the access definition menu:

- Access Code Entry, Access Code Definition, Elevator Definition
- Access Group Entry, Access Group Definition
- Access Override Entry
- Fail Soft Entry
- Project Definition

ACCESS CODE ENTRY [acdsentr]

Access codes are created using the access code entry [acdsentr] and the access code definition [acodentr] screens. A third screen, [eleventr], is used for elevator codes.

Three access code types are identified—Centralized (Host); Distributed; Smart Failsoft:

Centralized (Host) — Used when the host computer makes access decisions. An example is with global anti-passback, where in/out readers may be connected to different ACUs.

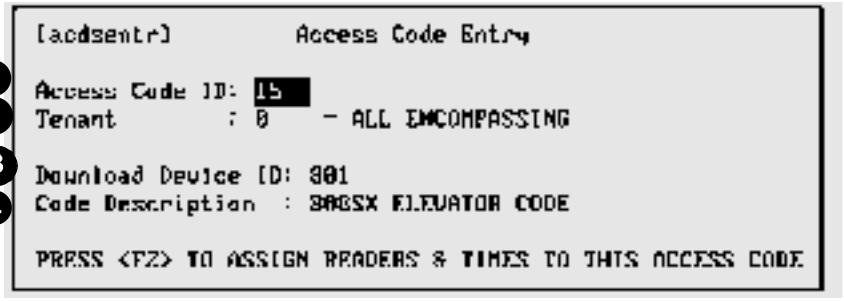
Distributed Access Codes — Distributed access codes are created for each ACU and are downloaded from the host. When a card is presented to a reader, the ACU makes the access decision. In some circumstances, the host computer may override an access request denied by an ACU.

Smart Failsoft — These codes work only if the ACU is in smart failsoft mode. This occurs when communication between the host and the ACU is interrupted for more than 15 seconds. During normal operation (ACU communicating with the host), access requests from keyholders with smart failsoft status are passed to the host for decision.

NOTE

Smart failsoft is not supported with 1050 keys used in conjunction with 708P and 718P ACUs, but a function is built in to the units which does provide some measure of failsoft protection in the event of a communications failure with the host. The ACUs can be programmed to accept up to 25 specific command keys, and access is allowed when these are presented (access may be for one to eight doors). The feature is limited to some extent in that time codes cannot be used in conjunction with this special programming, and event entries (door opening records, in this case) are not logged.

A sample [acdsentr] screen follows:



Access Code ID. Required. Enter a four-digit maximum access code number.

Tenant. Required (*zoom* available). Enter a four-digit maximum tenant code number. Default is tenant 0.

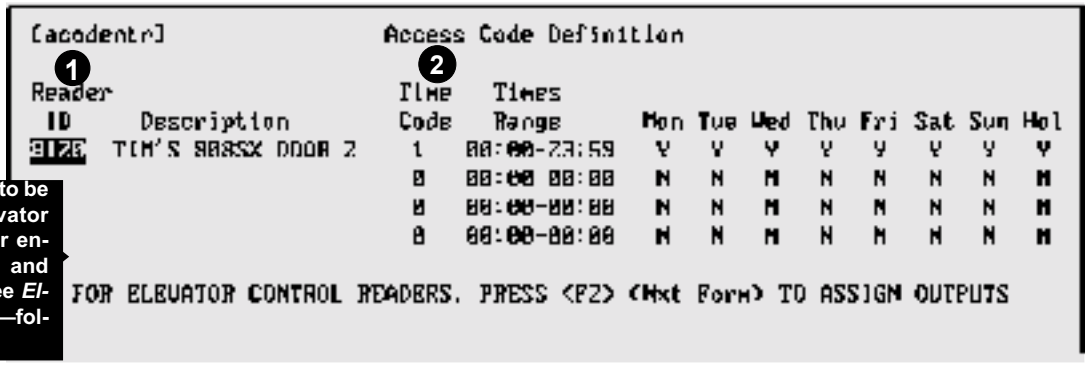
3 **Download Device ID**. Optional (*zoom* available). This field must be used if the access code being created is to be downloaded to an ACU—enter the ACU ID number. Enter **0** (default) if access decisions for this code are to be made by the host.

4 **Code Description**. Required. Enter a 30-character maximum description of the access code, e.g., REGULAR DAY SHIFT, WEEKEND RECEIVING.

When screen entry is completed press F6 to store the data; the access code definition screen, [acodentr], displays automatically.

ACCESS CODE DEFINITION [acodentr]

This screen is used to enter the reader ID and time codes (four maximum per reader) that will apply to this access code. Each reader ID entered must be added (F5) and stored (F6) individually. When you finish data entry for this screen, press F6 again to store the completed access code definition. A sample screen follows:



If this access code is to be assigned to an elevator reader, press F2 after entering the Reader ID and Time Code fields. See *Elevator Access Codes*—following subsection.

Note that this action may only be done for readers defined as elevator reader types in the reader definition screen.

Reader ID. Required. Enter the reader number to be linked to this access code (the reader description is automatically displayed). The reader numbers can be entered in any order.

Time Code. Optional. Enter up to four time codes, in any order, that apply to this access code (the time code parameters are displayed automatically). Default is 0 which is no access.

ELEVATOR DEFINITION [eleventr]

The elevator definition screen must be completed if the reader type is an elevator reader (reader type 5). Perform the following steps:

1. When the Reader ID and Time Code fields have been entered in [acodentr], press F2 to display the elevator definition screen [eleventr]—example below.

2. Enter the output contact IDs (usually wired to the elevator cab floor buttons) to be closed (activated) when access is granted via this reader. Store each item (F6) after entry. Use F5 to move to the next output contact ID line.

```
[eleventr]  Elevator Definition

  Reader/Point Id
           8004 = Contact 4
           8006 = Contact 6
           8008 = Contact 8
```

ACCESS GROUP ENTRY [agdsentr], [agrpentr]

To facilitate assigning similar access privileges to large numbers of keyholders, the system allows two or more access codes to be combined into an access group. Two screens are used: [agdsentr] and [agrpentr]. Sample screens follow.

```
[agdsentr]          Access Group Entry

Access Group ID  : 12
Tenant           : 2    = BETA COMPUTERS
Group Description: WEEKEND UNSKED TESTING
```

Access Group ID. Required. Enter a four-digit maximum access group number.

Tenant. Required (*zoom* available). Enter a four-digit maximum tenant number. Default is tenant 0.

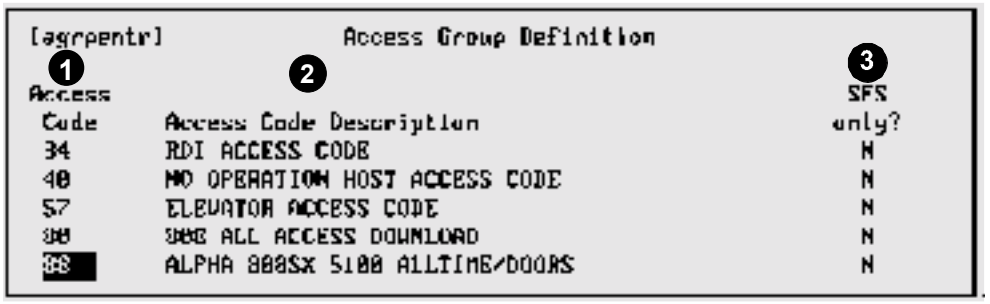
3 **Group Description**. Required. Enter a 30-character maximum description of the access group.

When screen entry is completed press F6 to store the data, at which point the *Access Group Definition* screen displays automatically. This screen permits you to enter the access codes that will apply to this access group. Each access code entered must be added (F5) and stored (F6) individually. When you finish data entry for this screen, press F6 again to store the now fully completed access group.

NOTE

Host-controlled and downloaded access codes may be combined in the same access group, but see *Warning* at the end of this subsection.

ACCESS GROUP DEFINITION [agrpentr]



Access Code. Required (*zoom* available). Enter an access code, in any order, to be linked to this access group. Each code must be added (F5) and stored (F6) individually.

Access Code Description. Automatically inserted by the system.

3 **SFS only?** (smart failsoft option). Optional. Smart failsoft access codes are used only when communications between the host and ACU are disrupted for more than 15 seconds. Enter Y if the downloaded access code is to be sent to the ACU as a smart failsoft access code. Note that this is used only in conjunction with host access codes. The default is N.

WARNING

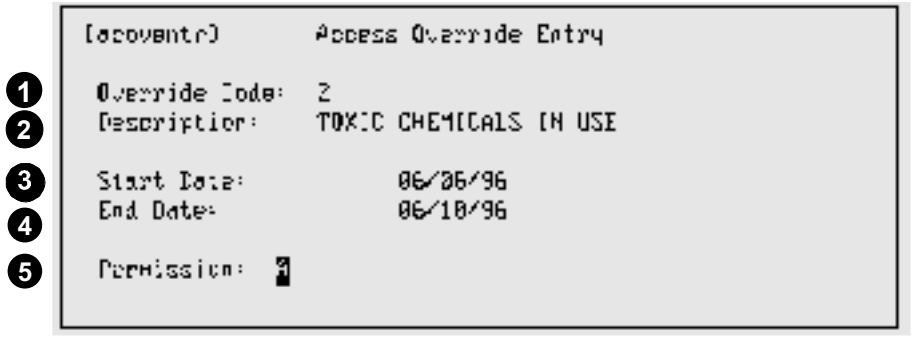
1. Access codes that include the same reader(s) should not be included in the same group unless one code is a downloaded code, and it has been set up with the SFS (smart failsoft) flag set to Y. Mixing codes that include common readers with different time codes may cause unpredictable results.

2. Do not combine two access codes with the same download device ID in one access group.

3. Keyholders may have only one downloaded access code per ACU.

ACCESS OVERRIDE ENTRY

Access override codes are typically used for visitors to restrict or allow access to specific locations for specific time periods. This is a host function that must be used only if normal access is through host access codes:



Override Code. Required. Enter an override code number in the range 1—9999.

Description. Optional. Enter a 30-character maximum description of the override.

3 **Start Date**. Required. Enter the override start date.

4 **End Date**. Required. Enter the override end date.

5 **Permission**. Optional. Permission status. Enter A to allow access; enter D to deny access. Default is A.

FAILSOFT ENTRY

708P ACUs can be programmed to recognize up to 25 keyholders (based on key numbers) for use when communication with the host computer is temporarily unavailable. Known as failsoft, the feature becomes active (access is granted) for these keyholders after 15 seconds following the occurrence of the communications interruption (response is not available for specific time periods, however). A sample screen follows:

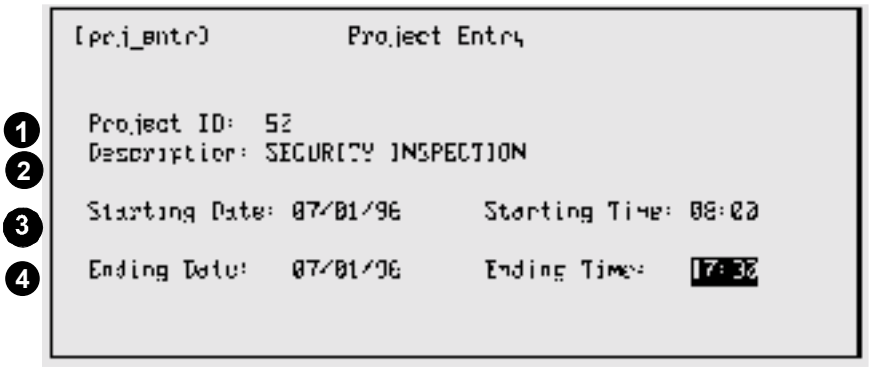
Device ID. Required (*zoom* available). Enter the device ID for which failsoft is to be assigned (the readers associated with the 708P automatically display).

Keyholder ID. Required (*zoom* available). Enter the applicable keyholder ID (keyholder name automatically displays).

3 **Allowed**. Optional. Enter Y or N as appropriate for the individual keyholder. Default is N.

PROJECT ENTRY [prj_entr], [prd_entr]

This is designed primarily for high security facilities. Project is used to grant temporary access to selected keyholders at project-controlled doors when a project is activated, while access for all other keyholders who normally enter through these doors is temporarily denied. The projects are continually monitored by the system and are updated as project status changes from activated to deactivated, and vice versa. This is a host function that must be used only if normal access is through host access codes. A sample [prj_entr] screen follows:



Project ID. Required. Enter a four-character maximum project ID code.

Description. Optional. Enter a 40-character maximum description of the project.

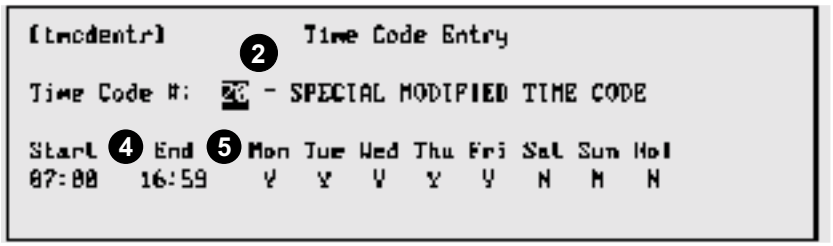
3 **Starting Date and Time**. Enter the project's starting date and time in the formats MM/DD/YY and HH:MM.

4 **Ending Date and Time**. Enter the project's ending date and time in the formats MM/DD/YY and HH:MM.

Store (F6) data when completed; the project definition [prd_entr] screen automatically displays. Enter the applicable reader IDs for this project (*zoom* available). Store (F6) each ID separately when entered, then immediately press F5 to move the cursor to the next data entry point on the screen. Repeat for as many readers as are to be included in the project. A sample [prd_entr] screen follows:

TIME CODES [tmcdentr]

Time codes are normally used to define when points and readers are active. The codes are also used to automatically lock / unlock doors, activate / deactivate output relays, and to initiate recurring tasks. When combined with readers into access codes, the time codes define when access is valid for particular readers. A sample [tmcdentr] screen follows:



Time Code #. Required. Enter a two-digit (maximum) time code. If the time code is omitted, the system defaults to time code 0 (zero). The default time code description is NEVER ACTIVE, with start/end times of 00:00 and N (no) for all the day entries.

= (description). Optional. Enter a 30-character maximum description of the time code.

3 **Start**. Required. Enter a start time using 24-hour notation with an intervening colon. Examples: 08:45 (8:45 a.m.), 19:15 (7:15 p.m.). If the start time is entered incorrectly, the system either prevents further data entry or displays an error message (press Enter to return to data entry). In both cases, reenter the time code using the correct format.

4 **End**. Required. Enter an end time All details for the Start field pertain.

5 **Mon through Hol**. Optional. The field represents the days of the week and holidays. Enter Y or N as applicable for the new time code. Default is N.

HOLIDAYS [hol_entr]

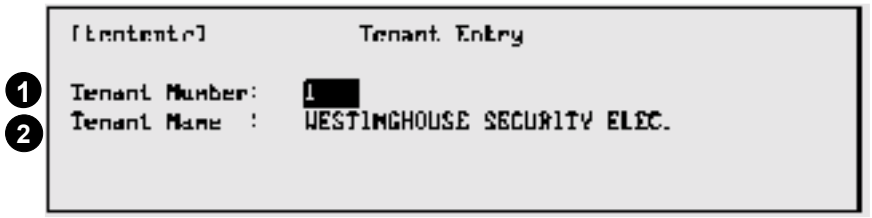
Annual holidays must be entered into the system. The information is required so that the host computer can determine whether access codes, auto-unlock functions, etc., need to be handled differently for the specified holidays.

Holiday Date. Required. Enter a date in the format MM/DD/YY (the system supplies leading zeroes where applicable).

Holiday Name. Optional. Enter a 20-character maximum holiday name.

TENANTS [tententr]

Two or more companies or groups can operate a single SE 6000 system, and they are referred to as tenants. (If required, the system can also be configured to allow individual tenants to share components.) Tenants may be unrelated occupants of the same or different facilities who use a single SE 6000 to view and manipulate only that data which applies to them. One of the tenants in a multiple tenant usage is the system owner who controls and has access to the entire system at all times. The systems owner may also be the system administrator. The default tenant code is 0 (zero), usually the system owner, who has access to the entire system at all times. A sample [tententr] screen follows.



Tenant Number. Optional. Enter a 4-digit maximum tenant number. Default is tenant 0.

Tenant Name. Optional. Enter a 30-character maximum tenant name.

INSTRUCTIONS [instentr]

Specific instructions are entered into the system to direct operators as to the action to be taken when a specific point is activated (usually in response to an activated alarm). The instructions display automatically on the alarm response screen, or may be selectively viewed from the realtime control maps. A sample [instentr] screen follows:

Point ID. Required (*zoom* available). Enter the point ID to which this instruction applies.

Tenant. The tenant number entered when this point was created is automatically entered into this field.

3 **Instructions**. Eight 40-character lines are provided for detailed instruction entry. Refer to the sample screen for an example.

HARDWARE CONFIGURATION [confmenu]

The hardware configuration item in the master file entry menu displays the hardware configuration menu [confmenu]:

- Zones
- Areas
- Pollers
- Devices
- Readers
- Points
- Auto Opens/Activates
- Device Report Definition
- SE 422 PIN Definition
- SE 422 Hardware Definition
- Dialer Entry
- Site Entry Definition
- ABA Configuration Entry
- DKR Configuration Entry

ZONES [ZONEENTR]

Zones comprise user-selected system components grouped to facilitate system operation and administration, and are required if the anti-passback feature is to be used. Zones may be defined for vehicles as well as keyholders. A sample [zoneentr] screen follows:

Zone Number. Required. Enter an four-digit maximum zone number. There is no default for this field.

Zone Name. Optional. Enter a 30-character maximum tenant name. If this field is omitted, the system fills the field with asterisks.

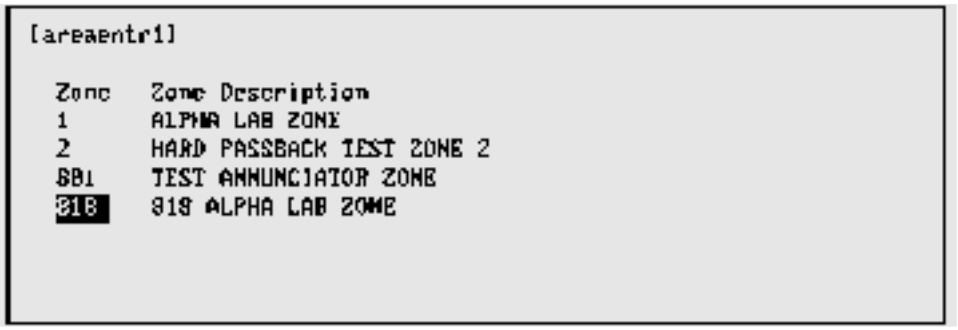
3. **Passback Area**. Optional. This field is used to indicate if passback is in effect for this zone. Enter P if personnel passback is used, V if vehicle passback is used, N if passback is not used. The default is N.

4. **Passback Type**. Required if passback (field #3) is either P (personnel) or V (vehicle) for this zone. Enter H for hard passback; S for soft passback. Hard passback prevents access if already in the zone; soft passback allows access and generates a passback violation message. There is no default for this field.

5. **Passback Level**. Required if passback (field #3) is either P (personnel) or V (vehicle) for this zone. Enter G for global (host-controlled); L for local (ACU-controlled). There is no default for this field.

AREAS [areaentr], [areaentr1]

For reporting purposes only, passback zones may be grouped into areas. Reporting (keyholder zone report) may be by zone or area, with the area report listing the zones contained in each area. Assign a number and optional description for the area using [areaentr]; enter the applicable zone numbers in [areaentr1]. Note that for local passback zones, ensure that both in and out readers are controlled by the same ACU. A sample screen showing [areaentr] and [areaentr1] follows:



POLLERS [pol_entr]

IMPORTANT

The pollers and poller parameter files discussed below are normally installed and tested at the factory or by your dealer. Please consult your dealer or WSE customer support before adding, changing, or deleting poller information.

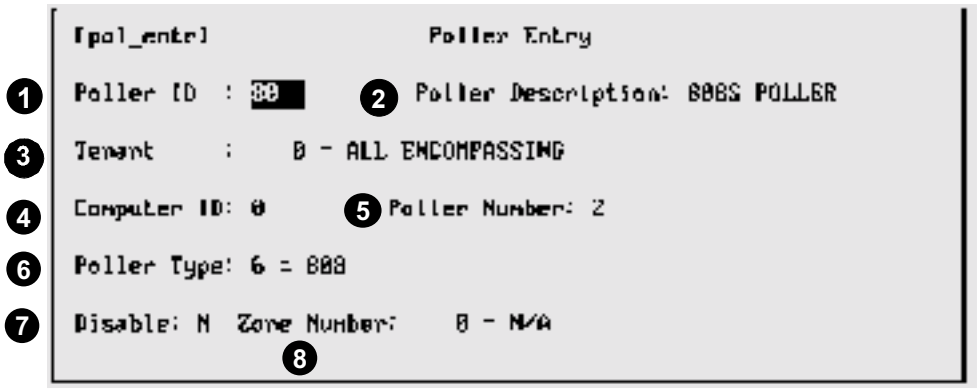
Pollers are device-specific application programs that communicate with the ACUs and the input / output controllers, and in addition to providing these communication links they perform many other tasks. For example, the pollers make access decisions, report devices that are not responding, and provide the means to reload devices with system and key data as necessary.

The SE 6000 can run different pollers or multiple copies of the same poller concurrently but, with the exception of the NexSentry, 8xx-series, and 422 ACUs, the pollers can be run with one device type only. Poller parameter files are read when the poller programs start. The parameters define the poller type, the physical port assignment, and other required control information.

Twenty-two poller types are currently in operation (codes 5, 20, 21, and 23 are not used):

1	708P	—	708P ACU
2	Opto	—	Optomux 22 alarm monitor
3	Etp - Rdu	—	Stellar RDU 2000 monitor
4	Timer Poller	—	Interactive extended processing poller
6	808	—	8xx series / SE 422 ACUs
7	MCCI	—	MCCI keypad
8	Parking	—	Parking controller—Internal: No physical connection
9	Remote Dialer Schd	—	Remote dial-up interface controller
10	Elevator	—	Elevator control poller—Internal: No physical connection
11	Database	—	Database poller—Internal: No physical connection
12	Burle	—	Burle closed-circuit television (CCTV)
13	Vicon	—	Vicon camera switcher
14	Hand Geometry	—	Supports up to 32 hand geometry readers
15	Amdi	—	Amdi 102 / 103 magnetic stripe readers (supports up to 16)
16	Radionics	—	6000/6500 Receiver
17	Nesting	—	Nested parking timer
18	Polaroid Server	—	Not used for Polaroid ID 4000
19	WSE XV Poller	—	Used for capturing images on an X-Terminal
22	WSE VIP2 Poller	—	Used with numeric keypad for entry of PINs
24	American Dynamcis	—	Closed circuit television (CCTV)
25	Pacom CCTV	—	Closed circuit television (CCTV)
26	Intercom System	—	Used to automatically switch cameras

A sample [pol_entr] screen follows:



Poller ID. Required. Enter a four-digit maximum poller number. There is no default for this field.

Poller Description. Optional. Enter a 20-character maximum description of the poller. If omitted, the poller ID number is inserted by default.

3. **Tenant**. Optional (*zoom* available). Enter a four-digit maximum tenant code number. Default is 0.

4. **Computer ID.** Required. Enter the ID of the computer on which this poller is to run. Default is 0—host computer.

5. **Poller Number**. Required. Enter the number of the corresponding poller-parameter file. Refer to the configuration sheet detailing the factory-assigned poller numbers.

6. **Poller Type**. Required. Use the zoom feature (F7) to access the Poller Type Display screen. Once there, arrow down to the required poller type, press F1, and the poller type number is entered automatically into the *Poller Entry* screen.

7. **Disable**. Not currently implemented.

8. **Zone Number**. Required. Enter a four-digit maximum zone number. Default is 0.

DEVICES

The most common devices used with SE 6000 system are the WSE NexSentry, 708P, 8*xx*-series and 422 ACUs. Other devices supported include:

- Opto 22 input / output controllers
- CCTV switchers
- Radionics alarm panels
- One or more additional SE 6000 systems used as local controllers

With the exception of the NexSentry, 8*xx*-series and 422 ACUs, each individual device type requires its own poller and associated hardware port assignment.

SIMPLE / INTELLIGENT DEVICE TYPES

The terms *simple* and *intelligent* are often used to describe certain device types used in conjunction with the SE 6000.

Simple Devices. With simple devices, the SE 6000 makes the access decisions and also instructs the device to take various actions. The 708P ACU is a simple device, for example.

Intelligent Devices. Depending on system configuration requirements, intelligent devices can be programmed to make their own decisions concerning access and actions to be taken. The devices typically have their own application software and / or firmware, and they maintain their own internal data files which are used for decision making. The NexSentry, 8*xx*-series, and 422 ACUs are intelligent devices, for example. As required, the intelligent devices can be set up to be

controlled exclusively by the SE 6000 (*deferred mode*), to operate entirely independently of the SE 6000 (*local mode*), or a combination of both.

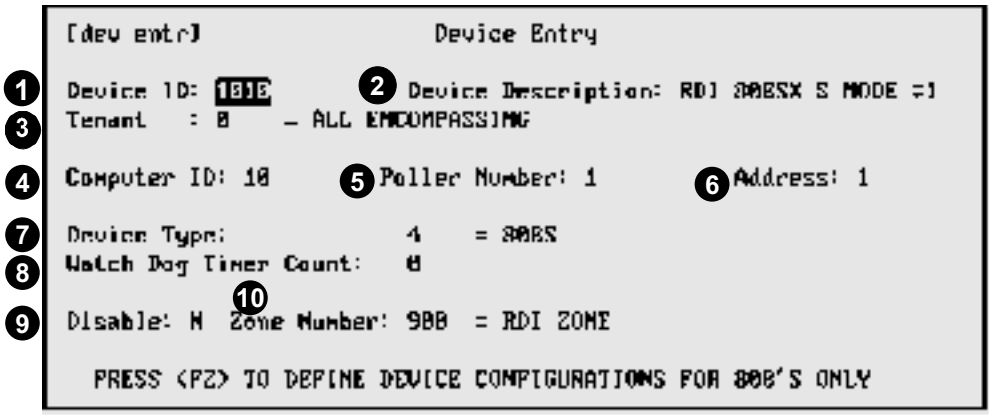
DEVICE ENTRY SCREENS

The following screens are used when setting up device types:

- 8xx-series ACUs — [dev_entr], [d808entr]
- NexSentry — [dev_entr], [nexsentr], [d818entr]
- 818-series ACUs — [dev_entr], [d808entr], [d818entr]
- 422 ACUs — [dev_entr], [d422entr]
- All other devices — [dev_entr]

DEVICE ENTRY [dev_entr] — ALL DEVICE TYPES

Complete the [dev_entr] screen when setting up any device. A sample screen follows:



Device ID. Required. Enter a unique, four-digit maximum device ID number in the range 1—9999.

Device Description. Optional. Enter a 20-character maximum description of the device. If omitted, the system enters the device ID number in this field.

3 **Tenant**. Optional (*zoom* available). Enter the tenant number applicable for this device. Default is 0.

4 **Computer ID**. Required. Enter the ID of the computer that connects to this poller. Default is 0 (host).

5 **Poller Number**. Required. Enter the number of the poller that connects to this device. This information is available from your system installer and should be obtained before beginning screen entry.

❻ **Address**. Required. Enter the address of the device. Since each poller can poll a number of devices, the *Address* field is necessary to tell the host which device to poll. The address ranges are included in the *Device Type* table (see following field). Note that the system will not allow duplicate device addresses on the same poller.

❼ **Device Type**. Required (*zoom* available). Enter the device type number in the range 1 through 23 (field 20 and 22 are not currently used):

Type	Description	Address Range (see previous field)
1	Host	1 only
2	Controller	1 — 8
3	708P	1 — 8
4	808S	1 — *16
5	Opto	0 — 15
6	Etp	1 — 16
7	MCCI	1 — 16
8	RDI	1 — 32
9	RLC	1 — 8
10	808SX/SN	1 — *16
11	818SX/SN	1 — *16
12	AMDI 102/103	1 — 16
13	NexSentry	1 — 16
14	Camera	1 only
15	SE422	1 — *16
16	Radionics	1 only
17	Polaroid ID 4000	1 — *16
18	818SC	1 — *16
19	808SXT	1 — 16
21	WSE VIP2	1 — 16
23	Timer Device	1 only

*Note that these are limited to 8 if used with host access.

❽ **Watch Dog Timer Count**. Required for Opto 22 devices only. Indicates the action to be taken if communication is interrupted between the host computer and the device. Enter:

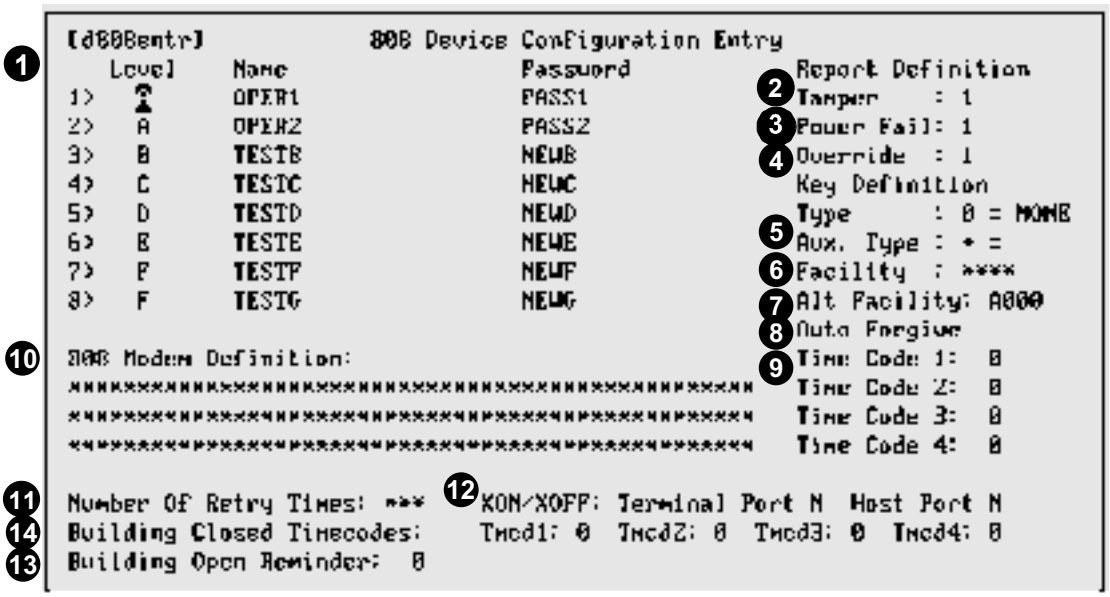
0 — No action (default)
1 — Open on time-out
2 — Close on time-out

❾ **Disable**. Required. A Y/N field indicating if the device is to be shunted at system start up (Y). This is recommended to disable devices until they are physically connected into the system. Default is N (device not shunted).

❿ **Zone Number**. Required (*zoom* available). Enter the zone number applicable for this device. Default is 0.

SE 8XX-SERIES DEVICE CONFIGURATION ENTRY [d808entr]

The [d808entr] screen must be completed for all 8*xx*-series ACUs (use F2 to display the screen after the previous screen has been stored). A sample screen follows:



Level, Name, Password. Required. These first three fields are entered to identify up to eight operators who will be permitted to set/change system parameters for a particular ACU from the ACU terminal port. User 1 must be established (defaults to operator 1); operators 2 through 7 are optional. Enter the operator's security code (A through F), name and password.

The security codes A through F control the degree to which the operator may add/change/delete the system parameters from the ACU terminal port. Code A has the most privileges, code F has the least. For detailed information concerning operator privilege levels, refer to the applicable ACU manual.

NOTE

The *Level*, *Name* and *Password* fields are specific to individual 804/808 ACUs and apply only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

Tamper. Optional. Enter the tamper report number if a report has been created (see applicable ACU manual). The report states the system actions that will be taken if the ACU enclosure housing is opened. Default is 0.

❸ **Power Fail**. Optional. Enter the power fail report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU should a power failure occur. Default is 0.

❹ **Override**. Optional. Enter the operator override report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU if, for example, a manual unlock or a shunt occurs. Default is 0.

❺ **Type**. Optional. Enter the number for the key type used. Default is 0.

NOTE

The valid key types are as follows:

0 — None
1 — 1030
2 — 1040
3 — 1050
4 — 1060
5 — 1050 / 1060 / Digital Keys

❻ **Aux. Type**. Conditional. Auxiliary key type. A second key type, other than the one entered in the previous field, can be entered here if applicable. Default is 0.

0 — None
1 — 1030
2 — 1040

Note: the previous two fields are applicable only to devices that support multiple key types.

❼ **Facility**. Required for key types 1 and 2 (previous field). Enter the facility code assigned to the keys. Defaults to **** if omitted.

❽ **Alt Facility**. Conditional. Enter a second facility code to allow a different set of keys to be used with this ACU. Defaults to **** if omitted.

❾ **Auto Forgive**. Optional. Up to four time codes can be entered that execute the forgive command at the ACU. Default is 0 (feature disabled if all auto-forgive time codes are 0).

❿ **808 Modem Definition**. Not used.

Number of Retry Times. Not used.

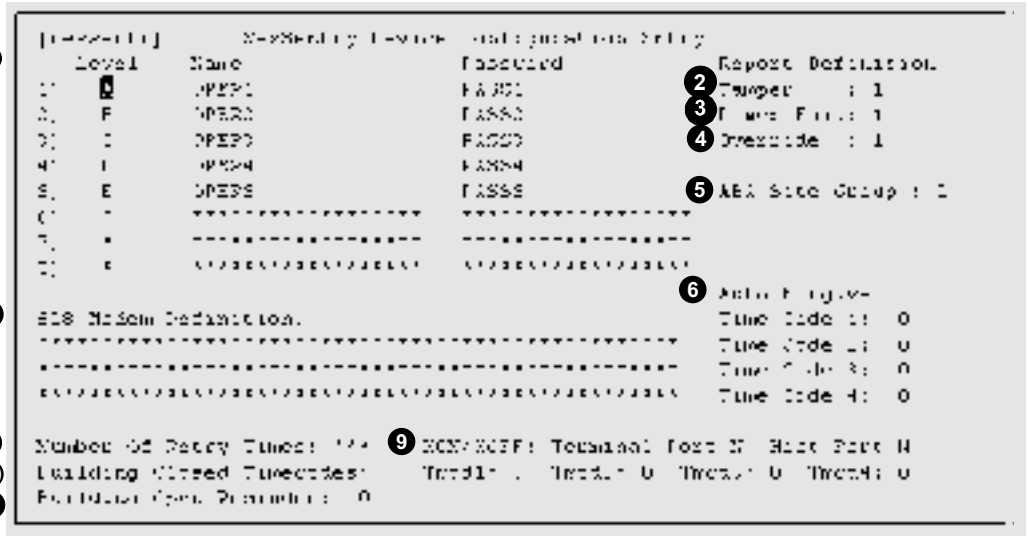
⓬ **XON/XOFF**. Not used.

13 **Building Closed Time Codes**. Optional. Provides up to four time intervals during which the building should be closed. Default is 0.

14 **Building Open Reminder**. Optional. If the building should be closed (indicated by the time codes entered in the previous field), a reminder message is logged and repeated for the number of minutes specified (0 to 240). Default is 0.

SE NEXSENTRY DEVICE CONFIGURATION ENTRY [nexsentr]

Complete the [nexsentr] screen for the NexSentry ACU and then press F2 Next Form to display the [d818entr] screen. Enter all appropriate information and press F6 Store to complete the NexSentry device configuration. A sample [nexsentr] screen follows:



Level, Name, Password. Required. These first three fields are entered to identify up to eight operators who will be permitted to set/change system parameters for a particular ACU from the ACU terminal port. User 1 must be established (defaults to operator 1); operators 2 through 7 are optional. Enter the operator's security code (A through F), name and password.

The security codes A through F control the degree to which the operator may add/change/delete the system parameters from the ACU terminal port. Code A has the most privileges, code F has the least. For detailed information concerning operator privilege levels, refer to the applicable ACU manual.

NOTE

The *Level*, *Name* and *Password* fields are specific to the NexSentry and applies only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

Tamper. Optional. Enter the tamper report number if a report has been created (see applicable ACU manual). The report states the system actions that will be taken if the ACU enclosure housing is opened. Default is 0.

3. **Power Fail**. Optional. Enter the power fail report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU should a power failure occur. Default is 0.

4. **Override**. Optional. Enter the operator override report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU if, for example, a manual unlock or a shunt occurs. Default is 0.

5. **ABA Site Group**. Optional. The ABA site code group ID number.

6. **Auto Forgive**. Optional. Up to four time codes can be entered that execute the forgive command at the ACU. Default is 0 (feature disabled if all auto-forgive time codes are 0).

7. **808 Modem Definition**. Not used.

8. **Number of Retry Times**. Not used.

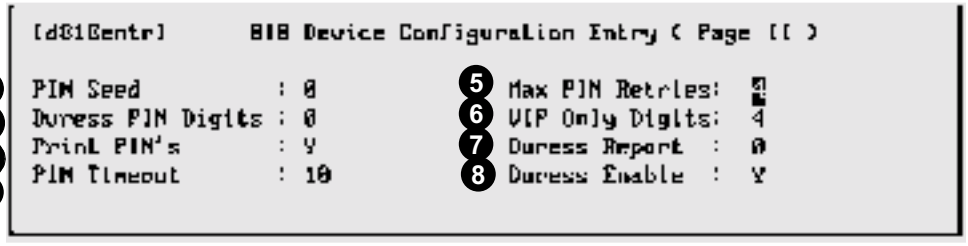
9. **XON/XOFF**. Not used.

10. **Building Closed Time Codes**. Optional. Provides up to four time intervals during which the building should be closed. Default is 0.

Building Open Reminder. Optional. If the building should be closed (indicated by the time codes entered in the previous field), a reminder message is logged and repeated the number of minutes specified (0 to 240). Default is 0.

SE 818 DEVICE CONFIGURATION ENTRY [d818entr]

Complete the [d818entr] screen for all 818-series and NexSentry ACUs (use F2 to display the screen after the previous screen, [d808entr] or [nexsentr], have been stored). A sample screen follows:



PIN Seed. Optional. Enter the base seed number for generating PINs. The value entered has priority over the system default PIN seed value entered with the [pndfentr] screen (see *SE 422 Pin Definition* in this section). Default is 0.

Duress PIN Digits. Optional. Enter the allowed number of digits for a PIN duress code. Default is 0.

3 **Print PINs**. Optional. A Y / N field indicating if the PIN should be displayed once calculated. Default is Y.

4 **PIN Timeout**. Optional. Enter the maximum number of seconds allowed between key presentation and PIN entry. Default is 10.

5 **Max PIN Retries**. Optional. Enter the allowed number of PIN entry retries. Default is 4.

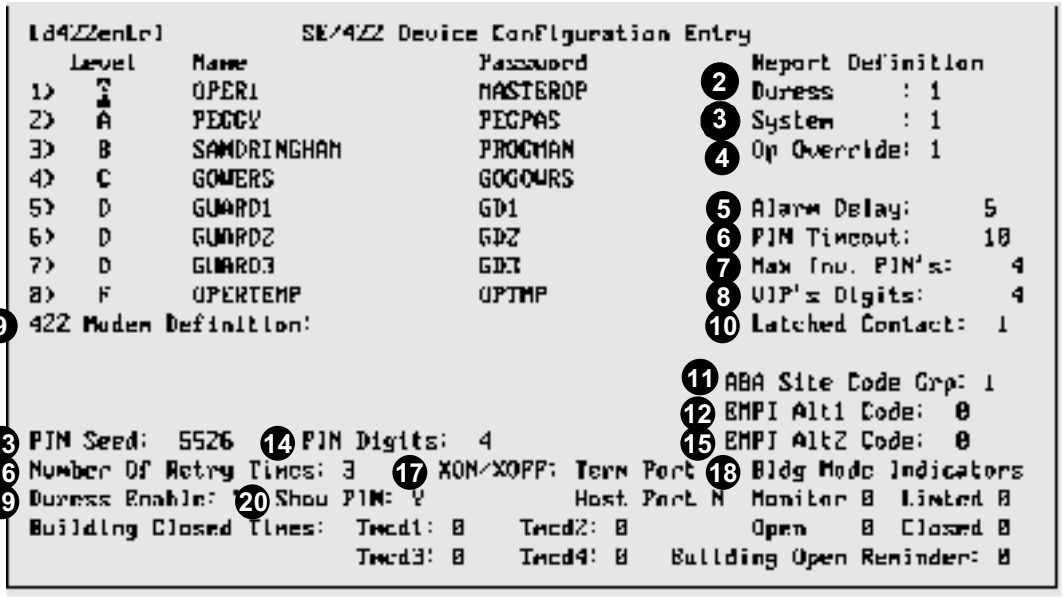
6 **VIP Only Digits**. Optional for keypad-controlled doors only. Enter the allowed number of digits for the PIN (4—8). Default is 4.

7 **Duress Report**. Optional. Enter an action report number (1—32) indicating the action the ACU is to take should a duress event occur. Default is 0.

8 **Duress Enable**. Optional. A Y / N field indicating whether the duress feature is enabled. Default is Y.

SE 422 DEVICE CONFIGURATION ENTRY [d422entr]

Complete the [d422entr] screen for SE 422 ACUs (use F2 to display the screen after the previous screen has been stored). A sample screen follows:



Level, Name, Password. Required. These first three fields are entered to identify up to eight operators who will be permitted to set / change system parameters for this particular ACU. User 1 must be established (defaults to operator 1); operators 2 through 7 are optional. Enter the operator's security code (A through F), name and password.

The security codes A through F control the degree to which the operator may add/change/ delete the system parameters. Code A has the most privileges, code F has the least. For detailed information concerning operator privilege levels, refer to the applicable ACU manual.

NOTE

The *Level*, *Name* and *Password* fields are specific to individual SE 422s and apply only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

Duress. Optional. A number (1-32) which instructs the SE 422 which action report to use should a duress event occur. Default is 1.

3 **System**. Optional. A number (1-32) which instructs the SE 422 which action report to use in response to system events in the SE 422. Default is 1.

4 **Op. Override**. Optional. A number (1-32) which instructs the SE 422 which action report to use in response to operator overrides performed on the SE 422. Default is 1.

5 **Alarm Delay**. Optional. The amount of time in seconds (10-240) that an alarm condition is allowed to exist before the alarm contact is closed. Default is 30.

6 **PIN Timeout**. Optional. The maximum amount of time, in seconds, which can pass between the presentation of a key and the entry of a verification PIN. Default is 10.

7 **Max Inv. PINs**. Optional. The maximum number of invalid PIN entry attempts to permit before cancelling the key presentation. Default is 4.

8 **VIPs Digits**. Optional. The number of digits in the PIN number for doors using keypads only. The range is 4 to 8. Default is 4.

9 **Modem Definition**. Not used when the SE 6000 is connected directly or in a dial-up configuration.

10 **Latched Contact**. Optional. The number of the output contacts that are assigned as a latched contact (0—51). Default is 0.

ABA Site Code Grp. Optional. The ABA site code group ID number.

12 **EMPI Alt1 Code**. Optional. Alternate EMPI site code #1.

13 **PIN seed**. Optional. The base seed number used when generating PINs. The value entered here has priority over the default PIN seed value entered on the [pndfentr] screen (see *Entering Default PIN Digits and Seed for an SE 422* in this section). Default is 0.

14 **PIN Digits**. The number of digits in the PIN code for this SE 422. The value entered here has priority over the default PIN digits value entered on the [pndfentr] screen (see *Entering Default PIN Digits and Seed for an SE 422* in this section). Default is 0.

15 **EMPI Alt2 Code**. Optional. Alternate EMPI site code #2.

16 **# of Retry Times**. Used to inform a remotely connected SE 422 the number of times to attempt to contact the host computer over telephone lines before considering a connection to be currently impossible to make.

17 **XON/XOFF**. Terminal Port and Host Port: Used to inform the SE 422 whether XON/XOFF flow control will be used at either of these two ports. Used for remotely connected SE 422s only.

18 **Bldg Mode Indicators**. Conditional. Enter the input point contact number or output relay number to initiate and display the status of the building mode.

Monitor — Input point contact ID (0 — 75)
Open, Limited, Closed — Output point relay ID (0 — 51)

19 **Duress Enable**. Indicates with a Y or an N whether the PIN duress feature of the SE 422 is turned on or not.

20 **Show PIN**. Indicates with a Y or an N whether the PIN number should be displayed on a local terminal connected to the SE 422 after it has been calculated.

Building Closed Times. Enter up to four time codes used for building closure.

Building Open Reminder. Enter the number of seconds (0 — 240) that the building open message is to display.

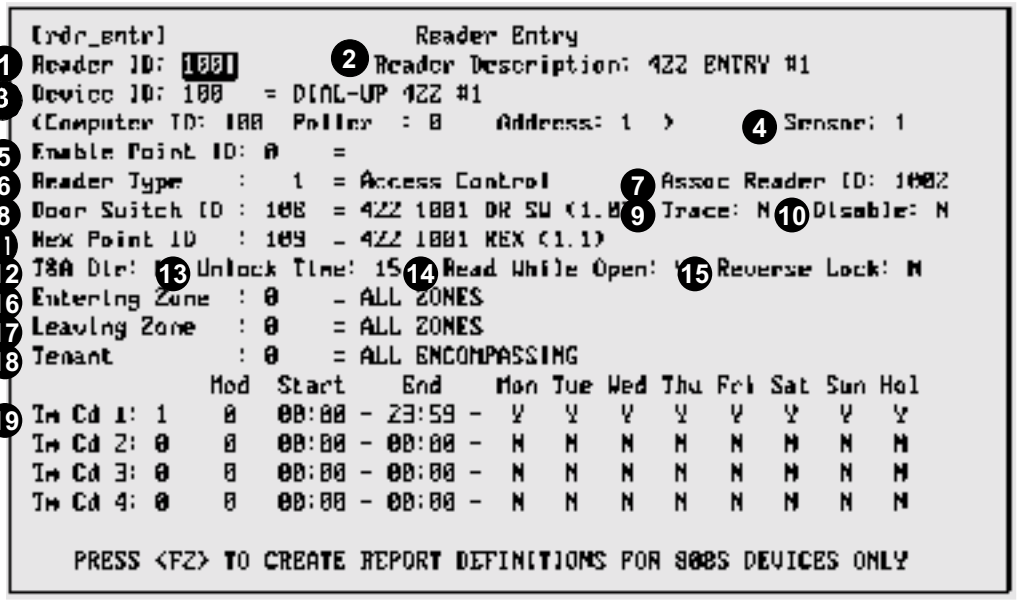
READERS

Readers are usually assigned to ACUs, but they may be used as standalone devices or linked to other security monitoring devices. Twelve reader types (1 — 12) are currently defined:

1. **Access Control**. Controls power to a door lock allowing or denying entry.
2. **Time and Attendance** (optional feature). Monitors keyholders' entry/exit movements.
3. **Meal Monitoring** (optional feature). Tracks number of meals taken by a keyholder.
4. **Guard Tour** (optional feature). Monitors guard check-in activities during guard rounds.
5. **Elevator Control**. Controls and limits keyholder access to floors.
6. **Activate** (optional feature). Enables keys for system wide use.
7. **Deactivate** (optional feature). Disables previously activated keys (see previous item).
8. **Auto Key Entry.** Allows automatic entry of card numbers.
9. **Access with Keypad**. Same as #1 except that a keypad is used in addition to the reader.
10. **Keypad**. Keypad only.
11. **Access with Two-Man Rule.** (optional feature). Same as #1 above except that two-man rule is in effect.
12. **MultiOcc Reader.** Multiple occupancy reader. Similar to #11 except that it requires that two keyholders enter and leave a zone together. Refer to the subsection that covers multiple occupancy readers in this section for more details.

Data entry begins with the [rdr_entr] screen. (One additional screen each is used for readers assigned to SE NexSentry, 8xx series, and 422 ACUs. Details follow this subsection.)

READER ENTRY [rdr_entr]



Reader ID. Required (*zoom* available). Enter a maximum four-digit reader ID number.

Reader Description. Optional. Enter a maximum 20-character description of the reader. Default is the reader ID number.

3 **Device ID**. Required (*zoom* available). Enter the number of the device which controls this reader. The related information (computer ID, poller number, address) automatically displays when the ID is entered.

4 **Sensor**. Required. Enter the sensor port number of the ACU to which this reader is connected.

5 **Enable Point ID**. Conditional (*zoom* available). Indicates a point ID that must be activated before the current point can be activated. Enter the enable point ID number.

NOTE

The **Enable Point** is primarily used with closed circuit television monitors, but can be used elsewhere. For example, a guard might need to personally recognize you and press an OK button (activates enable point) before your card will work at an ACU (current point). The system enters the default value of 0 (zero) if this field does not apply.

6 **Reader Type**. Required. Enter the reader type number in the ranges 1 through 12 as described above.

7 **Assoc Reader ID** (Associated Reader). Required if the reader is used in conjunction with a keypad. Enter the ID number of the Reader used with the keypad. Default is 0.

8 **Door Switch ID**. Required. Enter the door switch point ID used in conjunction with this reader. (If passback protection is in effect, two readers may share a single door switch.) The system enters the default value of 0 (zero) if this field does not apply.

9 **Trace**. A Y/N field used to indicate if all events at this reader are to be specially reported (traced). Default is N.

10 **Disable**. Required. A Y/N field indicating if the device is to be shunted at system start up (Y). This function varies with different types of ACUs. Default is N (device not shunted).

REX Point ID. Required if the reader is used in conjunction with a request-to-exit (REX) device or switch. Enter the REX ID number. The system enters the default value of 0 (zero) if this field does not apply.

12 **T & A Dir**. Time and attendance direction. If the time and attendance feature is used, enter N—None, I—Global In, or O—Global Out. The default is N.

13 **Unlock Time**. Optional for NexSentry, 8*xx*-series, and SE 422 ACUs. Enter a time period in seconds (1-240) that the door is to remain unlocked when a valid key is presented. Default is 10 seconds.

14 **Read While Open**. Optional for NexSentry, 8*xx*-series, and SE 422 ACUs. A Y/N field used to indicate if keys are to be read while the door is unlocked. The default is N.

15 **Reverse Lock**. Optional for NexSentry, 8*xx*-series, and SE 422 ACUs. A Y/N field used to indicate if the lock power is normally off (N) or on (Y).

16 **Entering Zone**. Optional. Enter the zone number for this reader, if applicable.

17 **Leaving Zone**. Optional. Used with anti-passback if reader controls exit from a zone. Enter the exit zone number.

18 **Tenant**. Optional. Enter a four-digit maximum tenant number. If omitted, Tenant 0 (zero - system owner) is entered by default.

19 **Tim Cd 1:** ... *and* **Mod**. Both optional. Four time codes may be entered denoting when this reader is active This function varies with different types of ACUs. Note that the downloaded ACU will still operate in the field during excluded time periods. If omitted, the reader is never

active. For **Mod**, enter a transaction modifier code (A, B, etc.) to customize log messages and system actions (see *Section 6: System Administration* for details). The default for Mod is 0 (zero); use the standard log message.

AUTO KEY ENTRY AND READER

The Auto Key Entry feature allows you to capture the key number from a key card and assign the number as well as enter the card number automatically in the Key Number field of the keyholder Entry [key_entr] screen. Before you can use this feature you must configure an Auto-Entry Reader (Reader type 8). Perform the following procedures:

- Configuring the Auto-Entry Reader
- Automatically Entering Card Numbers

Configuring the Auto Entry Reader

1. From the Main Menu, select Master File Entry and the Master File Entry screen appears.
2. Select the Hardware Configuration menu and the Configuration Menu [confmenu] screen appears.
3. Select Readers and the Reader Entry [rdr_entr] screen appears.
4. Select F5 Add Mode.
5. Enter all necessary information, making sure that you enter 8 in the Reader Type field.
6. Select F6 Store.

Automatically Entering Card Numbers

Note before you use the following procedure, you should configure an Auto-Entry Reader.

1. From the Main Menu, select Master File Entry and the Master File Entry screen appears.
2. Select Keyholders and the Keyholder Entry [key_entr] screen appears.
3. Select F5 Add Mode.
4. Enter the keyholders's ID, Last name, and first name and press Enter after each entry.
5. Position the key card next to the reader and at the beep, press F7 AutoKey.
6. Select F6 Store and select F5 Add Mode to enter additional Keyholders.
7. To enter additional keyholders, repeat steps 4 through 6.

MULTIPLE OCCUPANCY READER

The Multiple Occupancy Reader (MOR) is similar to a reader that is configured for the two-man rule requirement. The difference between them is that the multiple occupancy reader is also

configured for a specific zone and includes the passback feature. In addition, the MOR and the SE 6000 keep track of the people that are in a specified zone.

ENTERING A MULTIPLE OCCUPANCY ZONE

When a multiple occupancy zone is vacant, two keyholders are required to present their keys to the reader to unlock the door; first one and within a prescribed time period, the other, unlocking the door. Once three or more people are in the multiple occupancy zone, the reader works like a standard reader, that is, as an individual keyholder with rights presents their key, the door is unlocked, either entering or leaving.

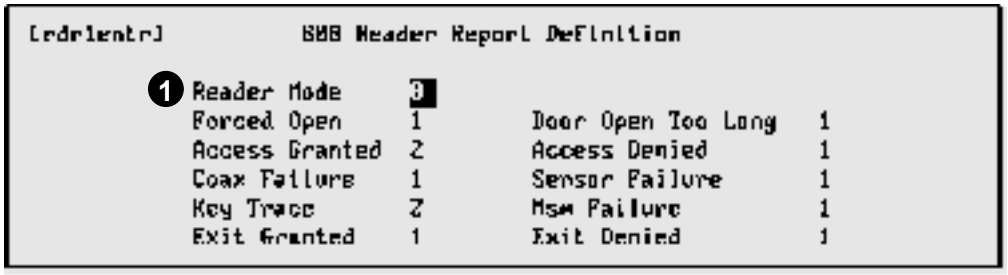
VACATING A MULTIPLE OCCUPANCY ZONE

Vacating a Multiple Occupancy zone, requires that the last two keyholders present their keys at the same time, first one and then within the prescribed time period the other, unlocking the door.

READER REPORT DEFINITION SCREENS

The reader report definition screens, [rdr1entr], [rdr2entr], [rdr3entr], and [rdr4entr] are used, respectively, when setting up a reader to operate with an SE 8xx-series, 422, or NexSentry ACU. Press F2 after storing the data on the [rdr_entr] screen; the appropriate second screen automatically displays.

SE 8XX-SERIES READER REPORT DEFINITION [rdr1entr]



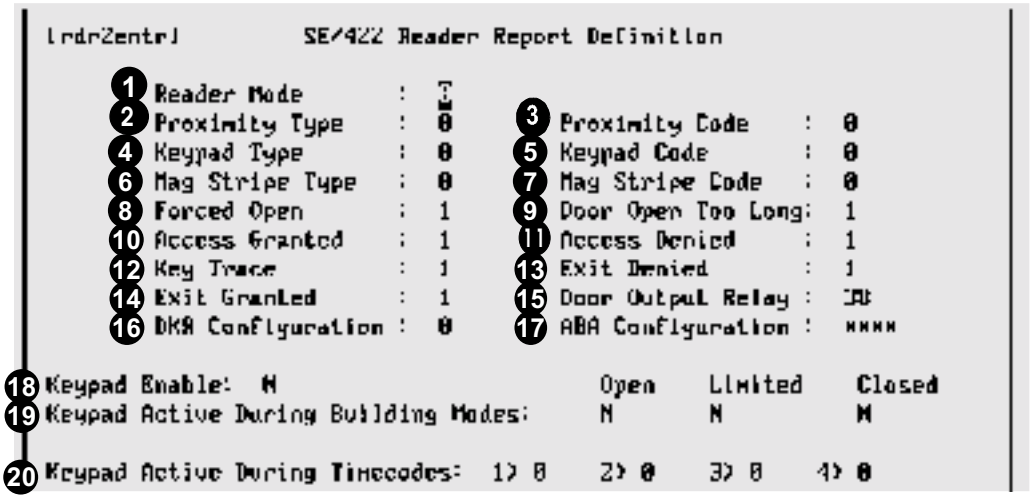
Reader Mode. Optional. Enter the appropriate reader mode number. This is used for building modes. The default is 0.

0 = Normal, 1 = Open, 2 = Closed, 3 = Station

The remaining fields, *Forced Open* through *Exit Denied*, require a report number entry. The word report in this context identifies a user-defined action or series of actions that the ACU is to take

in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in the section and the applicable ACU manual for detailed information.

SE 422 READER REPORT DEFINITION [rdr2entr]



Reader Mode. Optional. Enter the appropriate reader mode number: 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

Proximity Type. Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

3 **Proximity Code**. Enter the proximity reader node number: 0 = None, 15 = 1st proximity reader node number, 16 = 2nd proximity reader node number

4 **Keypad Type**. Enter the keypad type: 0 = VIP2, 1 = MSRK5.

5 **Keypad Code**. Enter the node number for the VIP keypad: 0 = None, 13 = 1st keypad node number, 14 = 2nd keypad node number.

6 **Mag Stripe Type**. Enter the magnetic stripe type: 0 = MSR, 1 = MSR5, 2 = MSRK5.

7 **Mag Stripe Code**. Enter the node number for the magnetic stripe reader: 0 = None, 17 = 1st magnetic stripe reader node number, 18 = 2nd magnetic stripe reader node number.

8—14

The following ten fields, **Forced Open** through **Exit Granted**, require the entry of a report number. The word report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in the section and the applicable ACU manual for detailed information.

15 **Door Output Relay.** Enter the number of the 422 relay.

16 **DKR Configuration.** Enter the ID number. Valid ranges of numbers is from 1-9999.

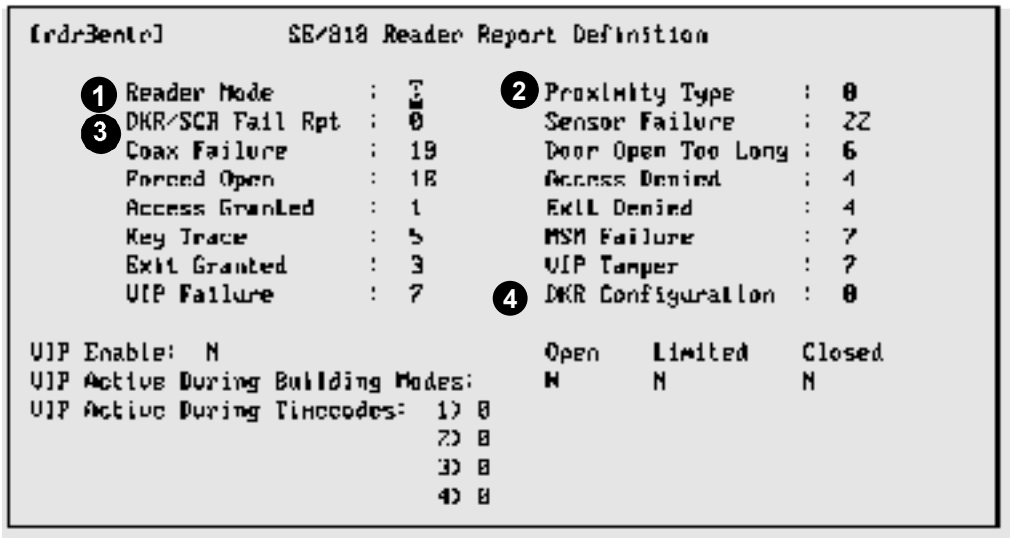
17 **ABA Configuration.** Enter the ID number Valid range of numbers is from 1-9999.

18 **Keypad Enable**. A Y / N field to activate the associated keypad.

19 **Keypad Active During Building Modes**. A Y / N field to indicate whether the keypad should be activated during the building open, limited and / or closed mode.

20 **Keypad Active During Time Codes**. Up to four time codes

SE 818 READER REPORT DEFINITION [rdr3entr]



Reader Mode. Optional. Enter the appropriate reader mode number. 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

Proximity Type. Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

3 The following thirteen fields, *DKR/SCR Fail* through *VIP tamper*, require the entry of a report number. The word report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in this section and the applicable ACU manual for detailed information.

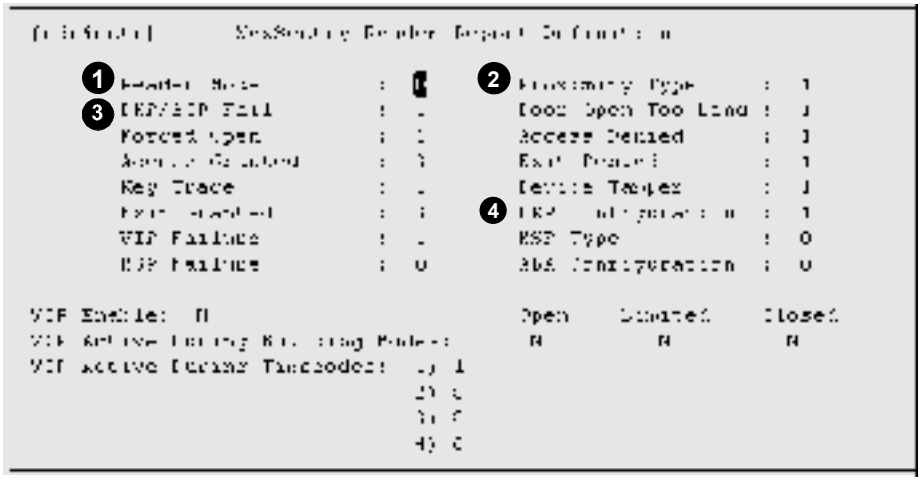
4 **DKR Configuration.** Enter the ID number. Valid range is from 1-9999.

5 **VIP Enable**. Optional. A Y/N/O field to enable/disable the VIP (O indicates VIP only). Default is N.

6 **VIP Active During Building Modes**. Optional. A Y/N field to activate/deactivate the VIP for building modes Open, Limited and Closed. Default is N for all three.

7 **VIP Active During Time Codes**. Optional. Enter up to four time code IDs when the VIP is to be active. Default is 0 for all four.

SE NEXSENTRY READER REPORT DEFINITION [rdr4entr]



Reader Mode. Optional. Enter the appropriate reader mode number. 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

Proximity Type. Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

3. The following eleven fields, DKR/SCR Fail through Device Tamper, require the entry of a report number. The report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See Device Report Definition in this section and the applicable ACU manual for detailed information.

4. **DKR Configuration.** Enter the ID number. Valid range is from 1-9999.

5. **VIP Enable**. Optional. A Y/N/O field to enable/disable the VIP (O indicates VIP only). Default is N.

6. **VIP Active During Building Modes**. Optional. A Y/N field to activate/deactivate the VIP for building modes Open, Limited and Closed. Default is N for all three.

7. **VIP Active During Time Codes**. Optional. Enter up to four time code IDs when the VIP is to be active. Default is 0 for all four.

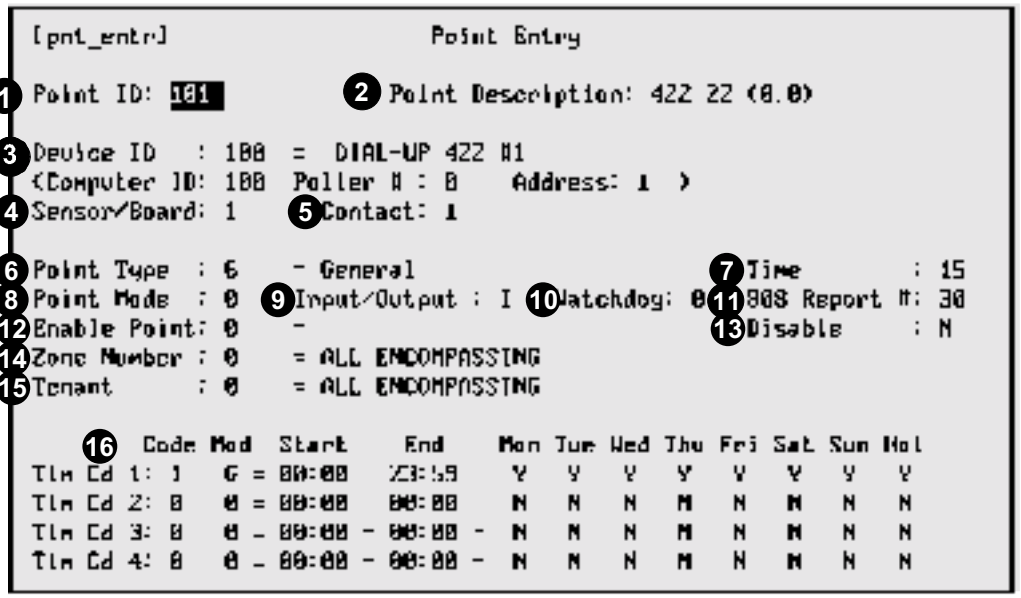
POINTS [pnt_entr]

Enter individual point IDs for all input and output points in the system.

Note:
There are eight hardware types (exclusively input and/or output contacts) that require a type number and a point number when being set up in the database. You establish these devices using the *Point Entry* screen and cause the log messages to differ depending upon point type:

1. **Alarm**. An input contact for monitoring conditions defined as alarms.
2. **Door Switch**. An input contact for determining the open/closed status of a door (only used when associated with a door record.
3. **REX**. An input contact for determining the status of a request-to-exit switch.
4. **Open On REX**. An input contact for determining the status of a request-to-exit switch which requires an action by the computer to unlock a specific door.
5. Not used.
6. **General**. An input or output contact for general purpose use. This function generates an input active message.
7. **Camera** (optional feature). Input / output contact for camera system monitoring and control.
8. **Spitter** (optional feature). Input contact to indicate a ticket pull for a parking control system.
9. **Guard Tour** (optional feature). An input contact allowing guard tour activity monitoring.

A sample screen follows:



Point ID. Required. Enter a four-digit maximum point ID number.

Point Description. Optional. Enter a 20-character maximum description of the point. If omitted, the system enters the point ID number into this field.

3 **Device ID**. Required (*zoom* available). Enter a four-digit maximum device ID number that is attached to this point. Once entered, the system automatically enters the associated computer number, poller number, and address fields.

4 **Sensor/Board**. Required. The sensor number or board number through which this point communicates. A point may be connected through a multiple switch monitor (MSM) to an ACU, or it may be connected directly to other device types. For an ACU, the number entered is the number of the sensor connection to the device. For devices with directly connected points (e.g., Optomux boards, alarm monitoring devices), enter 0 (zero), or the board number if multiple boards are connected on the same poller. Note that for WSE 422, 0 is for input points and 1 is for output points.

5 **Contact**. Required. For points connected through an MSM to an ACU, enter the MSM point contact number (1, 2, 3, or 4). For directly connected devices, enter the contact number for that device (0 through 15). Note for WSE 422, 0-75 is for inputs and 0-51 if for outputs. Refer to the WSE 422 input/output tables at the back of this section.

6 **Point Type**. Required (*zoom* available). Enter the point type number in the range 1 through 9 as described above, or screen-check using F7 (*zoom*).

❼ **Time**. Required for point type 2 (door switch) and 6 (general, when used with an OPTO 22); disregard for all other types. For type 2, enter the number of seconds before the door is to be considered held open. The range is 1 through 240 (the default is 15 seconds and this is the recommended value for normal usage). For type 6, and if this is an output point, enter the number of seconds that the OPTO 22 output remains active. The range is 0 through 655 (0 indicates no time limit).

❽ **Point Mode**. Required except for MSMs; enter 0 if this the case. Enter 0 (zero) if the point is normally open; enter **1** if the point is normally closed. Default is 0.

❾ **Input/Output**. Required. Enter **I** for an input point; enter O (letter O) for an output point. Default is I.

❿ **Watchdog**. Required for Opto 22 devices only. Indicates the action to be taken if communication is interrupted between the host computer and the device. Enter:

0 — No action (default)
1 — Open on time-out
2 — Close on time-out

808 Report #. Required for points attached to 8*xx*-series ACUs. Note that this is used with alarm generated points. If it is a door switch or a REX, it is defined on the second page of the Reader screen. The word report in this context identifies a previously-defined action that the ACU is to take in response to specific events. Up to 15 reports can be defined for each ACU (see the respective ACU manual for detailed information). Enter a number in the range 1 through 15 indicating the 808 report to be used. If omitted, Report #1 — report to host at all times — is used by default.

⓬ **Enable Point**. Conditional (*zoom* available). Indicates a point ID that must be activated before the current point can be activated. Enter the enable point ID number. This is only active for host control points.

NOTE

The *Enable Point* is primarily used with closed circuit television monitors (CCTVs), but can be used elsewhere. For example, in order to open a parking lot gate, a car must first be sensed by a detector (enable point). Then when the proper keyholder uses their key, the gate opens, allowing access.

⓭ **Disable**. Required. A Y/N field indicating if the point is currently disabled (Y). Default is N (point currently active). Note that an intelligent ACU will only control host action not the physical action at a site where the ACU reports a contact closure.

⓮ **Zone number**. Required (*zoom* available). Enter the zone number applicable for this point. The system enters the default value of 0 (zero) if this field does not apply.

⓯ **Tenant**. Required (*zoom* available). Enter the tenant number applicable for this point. The system enters the default value of 0 (zero - system owner) if this field does not apply.

⓰ **Tim Cd** (**1**-**4**), **Code** and **Mod**.

Code: Required (*zoom* available). Four time codes can be entered to allow input monitoring at this point. The default is time code #1.

NOTE

The system effectively shunts points and devices not covered by an active time code. Recommend controlling events through reporting when using an intelligent ACU.

Mod: Optional. Log messages and system action can be modified using the custom transaction modifier codes A, B, etc., (see *Section 6*, *System Administration*). Default is 0 and uses standard messages.

AUTO OPENS / ACTIVATES

The auto open / activate feature is used to instruct the system to lock / unlock doors, or activate / deactivate output points, for a predefined amount of time. Examples:

- A regular business door is configured to automatically unlock at a prescribed time each morning. The time code then re-locks the door at close of business each day.
- Via an output point, a time code automatically switches on an outside light each evening at a prescribed time. The same time code then automatically switches off the light at a prescribed time the following morning.

A sample screen follows:

Serial #. A nine-digit maximum control number automatically generated and displayed by the system when a new auto open / activate code is added. This information is not entered by the user.

Reader ID or Point ID. Required. Enter the applicable reader or output point ID number.

3 **Timecode**. Required. Enter the applicable time code.

Device Report Definition [rdefentr]

Use this feature to create action reports for the SE 8*xx*-series and SE 422 ACUs. An action report is a set of user-defined tasks performed by the ACU when specified conditions occur. The actions are defined using the device report definition screen (sample screen shown below); the reports are assigned using screens described in the device entry subsection. For complete descriptions on how to use the report definition screen for the various ACU types, please refer to the respective ACU manuals.

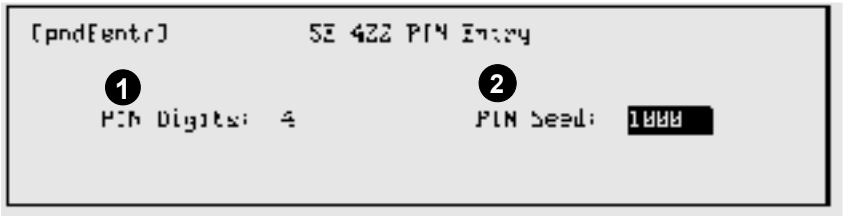
NOTE
The list of time conditions in the left hand side of the screen (Time Code A-C) and the task choices running left to right, such as Send To Host are used to define actions. To define an action, type a Y or N, or a number as appropriate for the desired task in the field under the appropriate task choice. For example, if you want the report to send information to the host when the building is in the open mode, type Y in the Bldg Open field under the Send to Host column.

```
[rdefentr]        Report Definition Entry

Device ID  001  = ALPHA LAB 600SX #10     Report #  4

                Send To Host   Close Latch  Close Output

Bldg Open       Y              N            N
Bldg Limited    N              N            N
Bldg Closed     N              N            N
Time Code A     1              0            1
Time Code B     0              0            0
Time Code C     0              0            0
Contact Num                                 4

Print Asterisk With Log  N    Prevent Bldg Closure  N
```

SE 422 PIN Definition

The number of PIN digits and the PIN seed must be defined and entered. The seed is used as part of an equation to calculate PIN numbers assigned to keyholders.

Assigned PIN numbers can be printed out (see *Section 3*, *SE 422 PIN Master Report*). Also, it is possible, but not recommended, to override the system-wide default values entered here (see *Device Entry*, SE 422, in this section). A sample data entry screen follows:



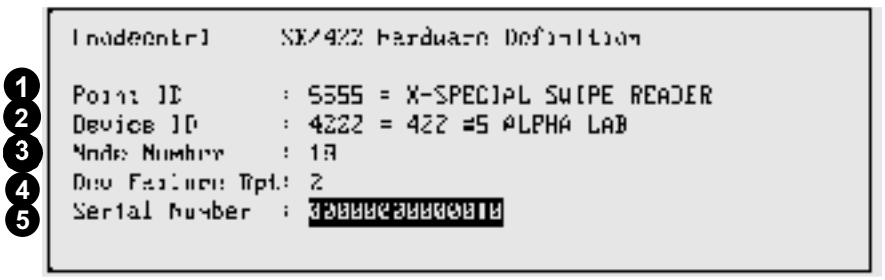
PIN Digits. Optional. Enter 4 or 5. Default is 4.

PIN Seed. Optional. Enter a number in the range 0 — 999999. Default is 0.

SE 422 Hardware Definition

Various special-function subdevices may be connected to the SE 422. These include input monitoring or output control devices (MIROs), proximity key or magnetic stripe card readers, and keypads allowing PIN entry.

The subdevices as connected to the SE 422 are known as nodes on the SE 422 communications network. A node is further defined by assigning it a point ID, by entering the device ID of the SE 422 to which the subdevice is attached, the communication address (node) number of the attachment, the report number to use if the device fails, and the serial number of the subdevice. A sample data entry screen follows.



Point ID. Required. Enter a four-digit point ID and device description.

Device ID. Required (*zoom* available). Enter an existing SE 422 device ID.

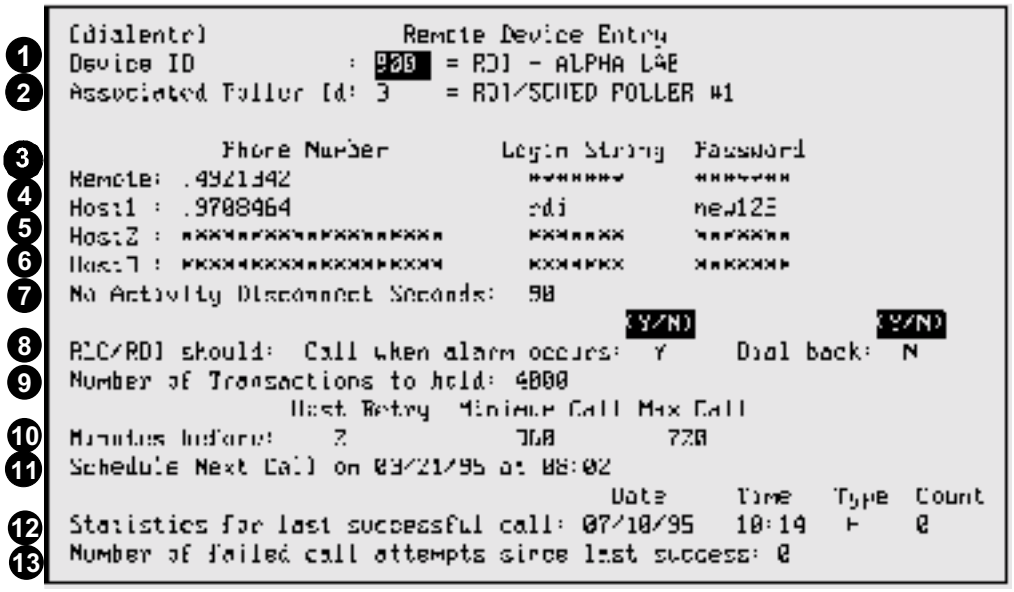
3 **Node Number**. Required. Note that each node device must have an address (or serial number) assigned to it with the Serial Command during database setup. Enter a node number in the range 1 — 18.

4 **Dev Failure Rpt**. Optional. Enter a device failure report number in the range 1 — 32. Default is 0 — No report.

5 **Serial Number**. Required. Enter the device serial number (imprinted on a rotary switch).

DIALER ENTRY

An optional, factory-set remote dial-up poller must be established to enable the remote dial-up feature for 8*xx*-series ACUs connect to an RDI unit or to a dial-up 422. The dialer entry screen is used to enter various control parameters for the off-site ACUs. A sample screen follows:



Device ID. Required (*zoom* available). Enter a four-digit device ID number (system automatically displays device description).

Associated Poller ID. Required (*zoom* available). Enter the remote dial-up (scheduler poller) poller ID number assigned to this device (system automatically displays poller description).

3 **Remote**. Required. Enter remote location phone number. Note that if the host must dial a prefix, be sure to include it.

4 **Host1**. Required. Enter host phone number. For RDI units only, enter log in string and password (default shown). Note that if the remote must dial an area code or other prefix, be sure to include it.

5. **Host2**. Required, if applicable. Enter alternate host #2 phone number. For RDI units only, enter login string and password.

6. **Host3**. Required, if applicable. Enter alternate host #3 phone number. For RDI units only, enter login string and password.

7. **No Activity Disconnect Seconds**. Optional. Enter the number of no activity seconds to elapse before host disconnects from the remote ACU. Default is 90 seconds.

8. **RLC/RDI should:** Two related Y / N fields:

   - **Call when alarm occurs:** Y or N
   - **Dial back:** Y or N — *Not currently implemented.*

9. **Number of transactions to hold:** Optional. Enter the number of transactions to be held in remote memory. Default is 4000.

10. **Minutes before:** Three related fields:

    - **Host Retry**. Number of minutes to wait before retrying call to host for example, every two minutes.
    - **Minimum Call**. Minimum elapsed time before dialing remote site for log messages (in hours) for example, every six hours.
    - **Max Call**. Maximum elapsed time before dialing remote site for log messages (in hours) for example, every 12 hours.

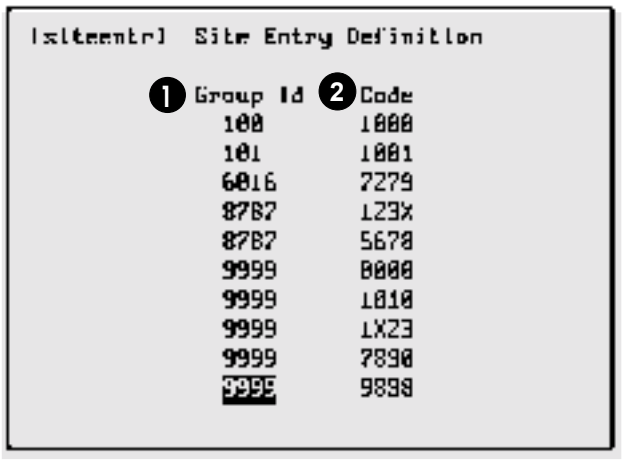
    Schedule Next Call on / **at**. Enter the time and date when next call is to be made. Note that a future date will cause the scheduler to Not dial the devices until the future date/tune is reached.

12. **Statistics for last successful call** (automatically displayed and updated): **Date**, **Time**, **Type**, **Count**.

13. **Number of failed call attempts since last success** (automatically displayed and updated).

Site Entry Definition

Site codes restrict the use of one or more doors to specific groups of cards (a particular company, a particular department, etc.). Up to 64 site codes can be assigned to the same card group ID. The group ID is used by ACUs which support ABA magnetic card readers to make access decisions based on site codes. A sample screen follows:

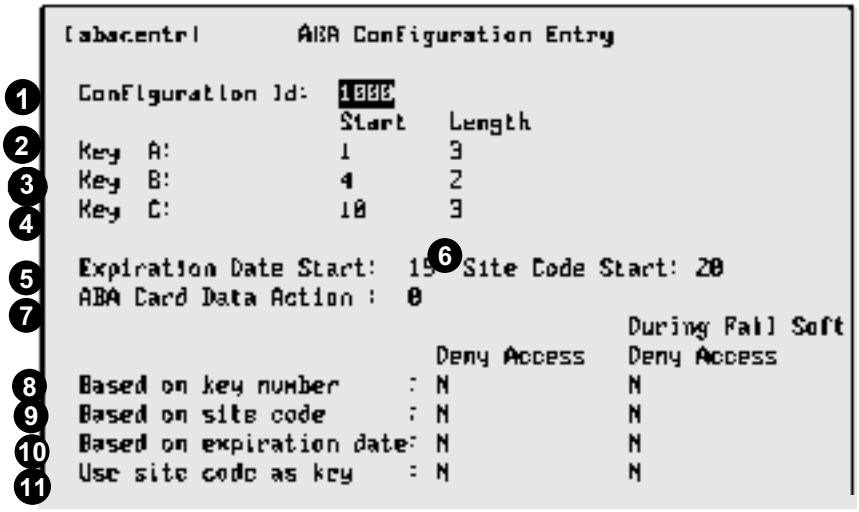


1 **Group ID**. Enter a four-character maximum group ID number.

2 **Code**. Enter a four-character maximum site code. Enter x in any position to act as a wild card; all characters in that position are matched. With the first 'x entry' in the sample screen, for example, the range 1230 through 1239 would be matched.

ABA Configuration Entry

The ABA (American Banking Association) configuration entry screen is used to define codes to be read from a standard ABA magnetic stripe card reader, and to define actions to be taken in response to the cards read. A sample screen follows:



1 **Configuration ID**. Enter a four-character configuration ID number.

2 **Key A**. Start position and length of first part of key. Key fields A, B and C are linked to form the key field.

3. **Key B**. Start position and length of second part of key.

4. **Key C**. Start position and length of third part of key.

5. **Expiration Date Start**. Expiration date start position.

6. **Site Code**. Site code start position.

7. **ABA Card Data Action**. The report number (ID) that will execute in response to an ABA card swipe event.

8. **Based on Key Number**. Y / N — Actions to take that are based on the key number.

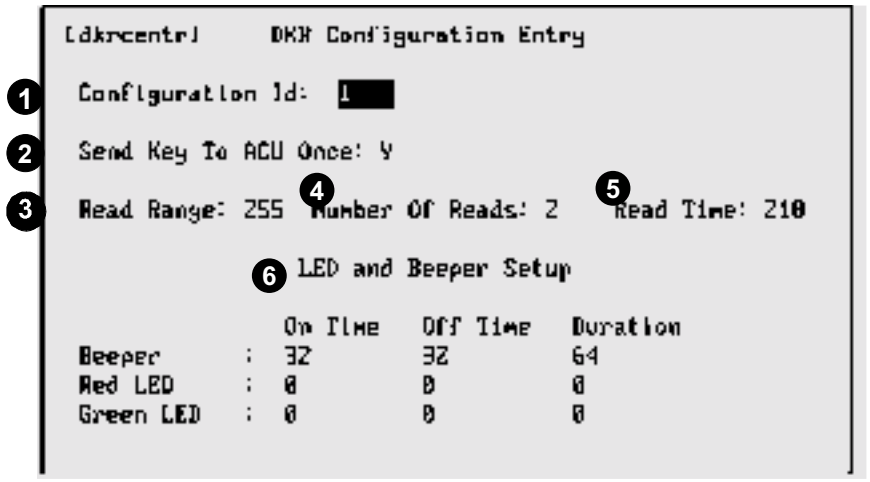
9. **Based on Site Code**. Y / N — Actions to take that are based on the site code.

10. **Based on Expiration Date**. Y / N — Actions to take that are based on the expiration date.

11. **Use Site Code as Key.** Y / N — Use the site code as the key number.

DKR Configuration Entry

The DKR (Digital Key Reader) configuration entry screen is used to change the factory-set operational default values. A brief introduction to these procedures is given here, but for complete information consult the appropriate DKR manual. *In all cases, however, do not attempt these procedures without first contacting your dealer and/or WSE customer support.*



Configuration ID. Enter a configuration ID number in the range 1 — 9999.

Send Key to ACU Once. Controls the number of times the key number is forwarded to the ACU while within the read-range of the reader. The default is Y—Once.

3. **Read Range**. Controls the maximum read range available with the particular digital reader. The range is 0—255; default is 255.

4. **Number of Reads**. Controls the number of additional verification reads of a single key within the sensor's range before declaring the key valid. The range is 0—255; default is 1.

5. **Read Time**. Controls the amount of time that the reader retains the key number in memory after the key is removed from the sensor's read range. The valid range is 0—65535 clock ticks (100 clock ticks is equal to 1 second); default is 100.

6. **LED and Beeper Setup**. Beeper, Red LED, and Green LED on-time, off-time, and duration. Override the default operation of the beeper, Red LED, and Green LED on the digital key reader in response to a valid key read. The valid range for on-time, off-time, and duration is 0-65535 clock ticks. The default is 0 (uses factory-set predefined behavior).

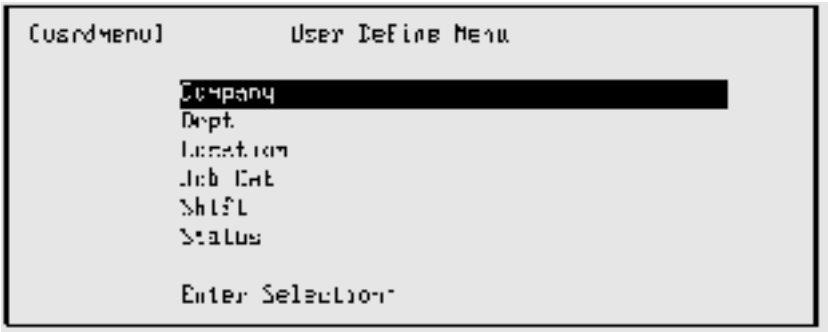
USER-DEFINED INFORMATION

Certain field titles on the keyholder record screens can be changed to suit the individual SE 6000 owner. Since keyholder records may be considered the primary data items for an access control system, many SE 6000 owners use the field title change feature to tailor the system to their precise requirements (these fields are provided for informational purposes and for use as report selection criteria, and have no effect on system processing).

The field titles are changed with the control file maintenance feature accessed from the System Administration menu (see *Section 6: System Administration*):

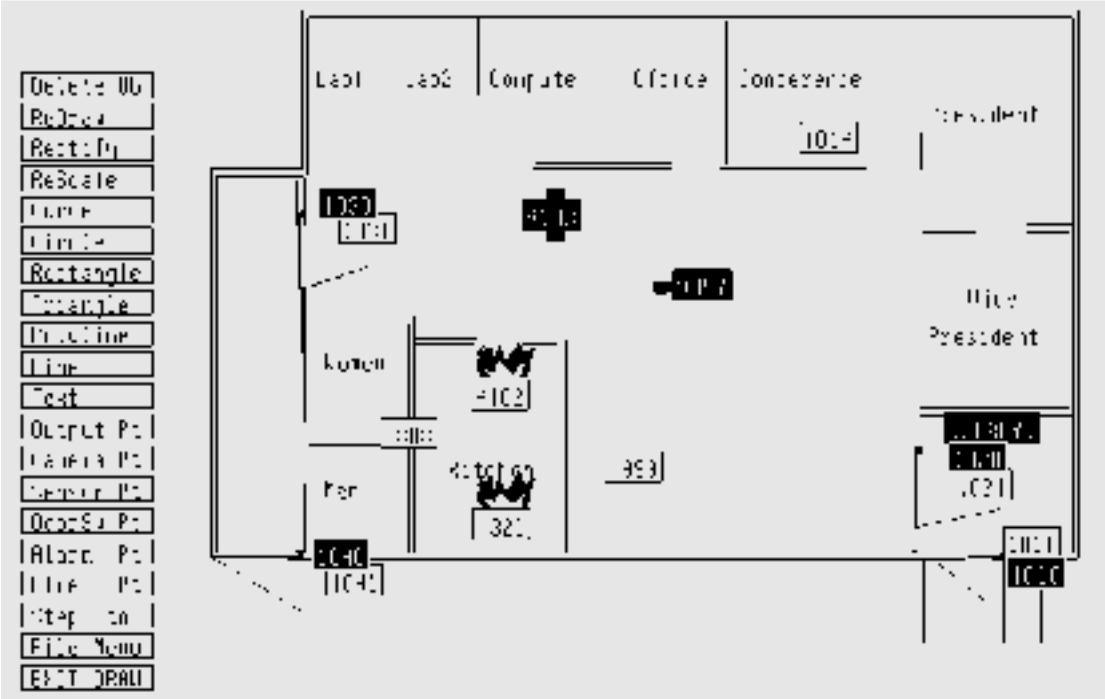
```
[ctrlentr]     Control File Maintenance

Company Name  Security Electronics

Field titles:  Enter "unused" for fields not required
  Fields on Page 1 of the Keyholder Entry screen:
    A:  Company       B:  Dept          C:  Location
    D:  Job Cat       E:  Shift         F:  Status

  Fields on Page 2 of the Keyholder Entry screen:
    1:  usr1          2:  usr2          3:  usr3
    4:  usr4          5:  usr5          6:  usr6
    7:  Remarks
```

The user-defined information selection here in the master file entry menu is used to assign descriptions to these fields. A sample screen follows: Note that a description of "unused" will skip the field during keyholder file maintenance.



MAPS

The DRAWMAPS function is used by the event monitoring function to display the location of doors, points, alarms, etc. To use this feature on an SE 6200 and above, it must be operating under the Reflection 4 terminal emulation software (mouse required). You can also use this feature on an SE 6100 or below from your console. This requirement is due to the SCO Unix graphic memory limitation. The function has several built-in HELP maps, and drawing instructions display at the foot of all screens. A sample map follows:



MAP DRAWING COMMANDS AND DESCRIPTIONS

COMMAND	DESCRIPTION
Delete Ob	Remove graphics and text. Once selected, the menu list shows only those object types currently on the map. Select one, then follow deletion instructions.

ReDraw	Redraws screen. Use if graphics appear incorrect.
Rectify	Makes all lines *close* to horizontal or vertical *exactly* horizontal or vertical. Lines *nearly* 45° are drawn at *exactly* 45°.
Rescale	Rescale (resize) map. Lines and curves change; text and icons do not change.
Curve	Draw curved lines.
Circle	Draw circles.
Rectangle	Draw boxes.
Triangle	Draw triangles.
Polyline	Draw connected lines.
Line	Draws a single line.
Text	Create text labels (large and small).
Outpt Pt	Output point icon — Rectangle with a smaller rectangle crossing it (point 4103 on sample map).
Camera Pt	Camera point icon — Rectangle with a small projection to the left (point 9997 on sample map).
Sensor Pt	Sensor point icon — Black rectangle when locked; white when unlocked (point 1030 on sample map).
DoorSw Pt	Door switch icon (point 1031 on sample map).
Alarm Pt	Alarm point icon — Red rectangle (point 999 on sample map).
Fire Pt	Fire point icon. The icon shows a red and yellow flame above a rectangle (point 4102 on sample map).
File Menu	Switch to File Menu to load, save, rename, copy, delete, or start new maps.
EXIT DRAW	Exit DRAWMAPS program.

SE 422 Input Table

		0	1	2	3	4	5	6
ACU (2-state)	0:	1	2	3	4	5	6	7
M16 /RO1	1:	8	9	10	11	12	13	14
(4-state input)	2:	15	16	17	18	19	20	21
	3:	22	23	24	25	26	27	28
	4:	29	30	31	32	33	34	35
	5:	36	37	38	39	40	41	42
	6:	43	44	45	46	47	48	49
	7:	50	51	52	53	54	55	56
	8:	57	58	59	60	61	62	63
RO4 (4-state)	9:	64						
	10:	65						
	11:	66						
	12:	67						
VIP (2-state)	13:	68						
	14:	69						
SI (4-state)	15:	70	71					
	16:	72	73					
MSR (2-state)	17:	74						
	18:	75						

Input points are always on sensor 1, contact 1-75

SE 422 Output Table

		0	1	2	3	4	5
Acu (2-state)	0:		1	2	3	4	5
M16/RO1	1:	6	7				
(4-state input)	2:	8	9				
	3:	10	11				
	4:	12	13				
	5:	14	15				
	6:	16	17				
	7:	18	19				
	8:	20	21				
RO4	9:	22	23	24	25	26	
	10:	27	28	29	30	31	
	11:	32	33	34	35	36	
	12:	37	38	39	40	41	
VIP	13:		42	43	44		
	14:		45	46	47		
SI	15:						
	16:						
MSR	17:		48	49			
	18:		50	51			

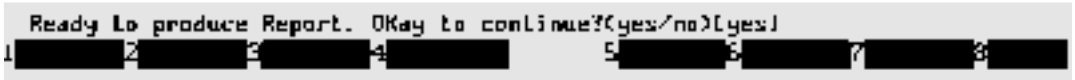
Output points are always on sensor 2, contact 1-51

SECTION 5
MASTER FILE REPORTS

INTRODUCTION

The master file reports list comprehensive database information. The report menu screens are accessed via the master file reports menu [rprtmenu], displayed via the main menu. In this section, the reports are documented following the reports menu sequence (see section table of contents). A sample [rprtmenu] screen follows:

All screens in this section show the system default values, with most screen fields requiring a numeric range entry. For example, the default range for keyholders is 1 — 999999999 (to reduce waiting time while a report is generating, enter the smallest range of numbers for each category which will still provide the information wanted). Other screen fields include choices for date ranges, regular or extended information, and report sequencing. When all fields have been entered, press Enter (Yes - default) to begin report generation:



Once compiled, a report output selection displays. Normally, 1 (system report printer) or D (display at terminal) is chosen. The system also gives the option to print to a terminal printer. Report totals are printed at the end of each report.

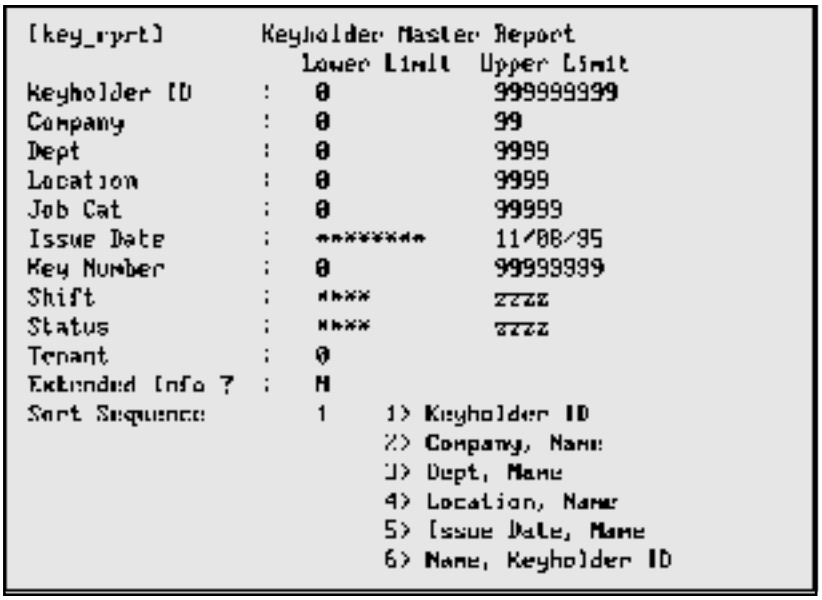
ADDITIONAL INFORMATION

An additional report feature not accessed via the reports menu, *132-xx Column Report Display*, is detailed at the end of this section.

KEYS MASTER

Two versions of the keyholder master report are available — Keyholder Quick List and Keyholder Master List (extended). The quick report includes keyholder ID, key number, keyholder name, information from user-defined fields B and D, phone number, title, user-defined field C, and floor. The master report includes all the keyholder information entered on page 1 of the keyholder entry screen, plus address, phone number, and user-defined field 7. Also, the master report prints access code information (first 20 codes) for each keyholder. A sample [key_rprt] screen follows:

Note that certain report screens include a sort sequence field and a numbered list of sort sequence categories. Enter one of the numbers into this field to print data related to that sequence number. For example in the Keyholder Master Report screen, enter number 1 in the Sort Sequence field to sort data by keyholder ID (see the following example).



KEYHOLDER QUICK LIST — SAMPLE REPORT

```
06/02/96                              BAYOU INDUSTRIES                  Page    1
14:45                                 Key Quick List

KeyholderKey No    Keyholder Name          Dept.  Pos.  Phone     Title                      Bldg
-------------------------------------------------------------------------------------------
   220774  409     JENSEN STEVE            11     6                                        18
   221922  811     KREBS SCOTT             11     6                                        18
   222172  512     DUNN JEFF               11     7     123-4567                           18
   233132  588     NEWMAN TERESA           11     0     890-1234  RECEPTIONIST             18
   239445  277     CLEMENT KAREN           11     0                                         5
   245165  338     KIRK KATHY              11     6               PINKERTON SECURITY       18
   246763  445     FERRELL STUART          11     7     567-8901  SECURITY MGR             18
   247666  176     KERR KATIE              11     0                                         0
   248112  765     LOWE LORRAINE           11     7     234-5678  SECURITY RECEPTIONIST     2
   249343  453     GREENWOOD LORI          11     7     901-2345  SECURITY RECEPTIONIST     1
```

KEYHOLDER HOLDER MASTER REPORT — SAMPLE REPORT

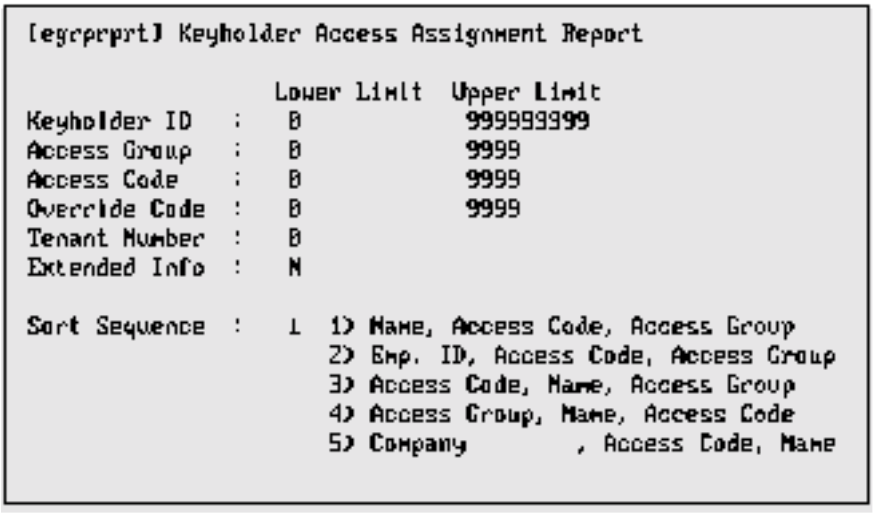
```
08/02/96                                McArthur Complex
PAGE               1
10:58                                   Keyholder Master List

Keyholder    222541  Name       Cross, Gregory             Company      2 = J o h n s
Lynne        Company
Key No         2332  Addr1      1917 Blair Avenue          Dept         2 =
Engineering
S.S. No 123-45-6789  Addr2      Weston, CA 95199           Location     5 = S a n t a
Clara Annex
Tenant            1  Addr3                                 Job Cat     14 = Software
Engineer
P.I.N.         1314  Privledge  YES                        Shift        0 = N/A
Remarks  Occasional late evening, weekend work             Status       0 = N/A
Phone (123)456-7890 Trace N  Visitor YES  Issued 07/14/96 Returned **********
Access Codes   1   4   7   8   21
```

ACCESS ASSIGNMENTS

KEYHOLDER ACCESS ASSIGNMENT

This report prints the access codes and access groups assigned to keyholders. Regular and extended versions of the report are available.

The regular report lists keyholder numbers and names, access code / group numbers and descriptions, and access override codes where applicable. The extended report includes this data and also gives key number, social security number, tenant number, PIN, company, department, location, job category, shift, status, remarks, phone, trace, visitor, and badge issue information. A sample screen follows:



KEYHOLDER ACCESS ASSIGNMENT: REGULAR — SAMPLE REPORT

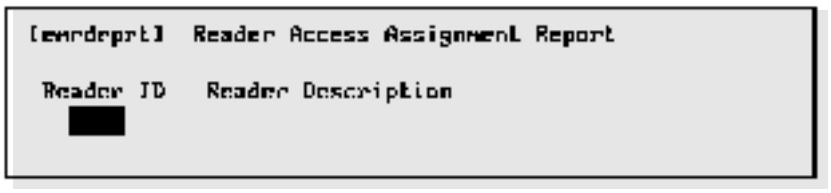
```
06/06/96                              BARON PARK HOLDINGS                    Page    1
10:13                                 Keyholder Access Assignment List

Keyholder  Keyholder Name          Code  Code Description       Group  Group Description  Override
_________  ____________________  _____  ____________________  _____  _________________  ________
    23342  Smith, James               1  Host 422, 708, 818        1  Main                  0
    22243  Stevens, Sandy             1  Host 422, 708, 818        1  Main                  0
    21188  Svensen, Lars              1  Host 422, 708, 818        1  Main                  0
    23397  Swenson, Lawrence          1  Host 422, 708, 818        1  Main                  0
    24411  Tauber, Linda              1  Host 422, 708, 818        1  Main                  0
```

KEYHOLDER ACCESS ASSIGNMENT: EXTENDED — SAMPLE REPORT

```
06/09/96                          Nova Systems, Inc.                        Page  1
12:30                             Keyholder Access Assignment List

Access Code 1 = Host 422, 808, 818              Override Code  0 =
Keyholder      331  Name         Sands, Jerry                  Company   1  = Nova Systems
Key No        1038  Addr1        1727 Oakmead Parkway          Dept      3  = Engineering
S.S. No987-65-4321  Addr2        Apt 12B                       Location  1  = Tulip Grove Main
Tenant           1  Addr3        Tulip Grove, CA 91999         Job Cat   6  = Software Engr
P.I.N.        2198  Privledge YES                              Shift   0    = N/A
Remarks                                                       Status  0    = N/A
Phone  224-8089 Trace NO  Visitor NO   Issued 03/31/95 Returned ***********
```

READER ACCESS ASSIGNMENT

This report prints keyholder access permissions at a specific reader and applicable time codes. A sample screen follows:



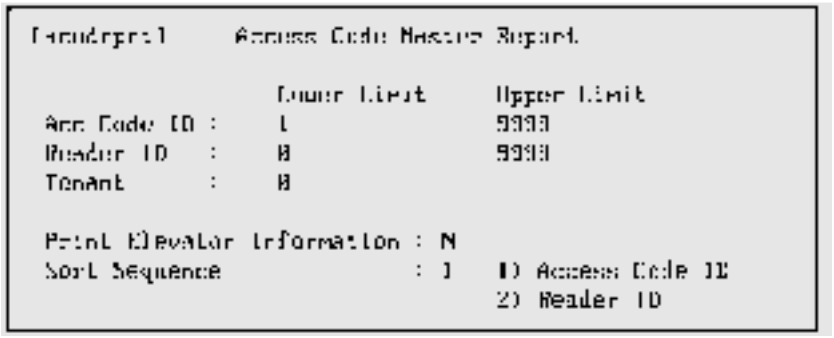
READER ASSIGNMENT — SAMPLE REPORT

```
04/16/96                          Soames Industries                          Page   1
11:26                             Access Report by Reader

Keyhld Id Keyholder Name    Reader  Reader Description Tmcd  Start End   Mon  Tue  Wed  Thu  Fri  Sat  Sun  Hol
--------- ----------------------- ------ ------------------ ---- ----- ----- ---- ---- ---- ---- ---- ---- ---- ----

   12235 Honsleigh Paul        57  Freight Car #3     1    00:00 23:59  Y    Y    Y    Y    Y    Y    Y    Y

   12345 McDermott Ian         57  Freight Car #3     1    00:00 23:59  Y    Y    Y    Y    Y    Y    Y    Y

   13445 Allentown Debra       57  Freight Car #3     1    00:00 23:59  Y    Y    Y    Y    Y    Y    Y    Y
```

ACCESS DEFINITION

ACCESS CODE MASTER

This report details all access codes defined in the system (the report can be limited to a single code or a range of codes, as required). A sample screen follows:



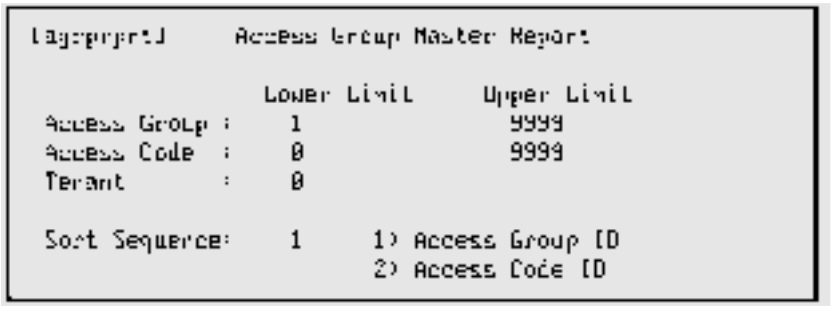
ACCESS CODE MASTER LIST — SAMPLE REPORT

05/02/96 Soames Industries Page 1
11:26 Access Code Master List

Code	Code Description	Reader	Reader Description	Tmcd	Start	End	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Hol
12	Weekend Rcvng	22	Receiving #1	14	09:00	15:00	N	N	N	N	N	Y	Y	N
13	Holiday Rcvng	22	Receiving #1	15	09:00	12:00	N	N	N	N	N	N	N	Y
19	Lab After Hrs	06	Lab Main	05	15:30	23:59	Y	Y	Y	Y	Y	N	N	N
20	Lab Weekends	06	Lab Main	06	09:00	23:59	N	N	N	N	N	Y	Y	Y

ACCESS GROUP MASTER

This report details all access groups defined in the system (the report can be limited to a single group or a range of groups, as required). A sample screen follows:

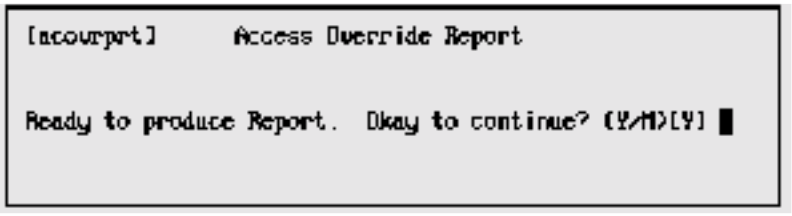


ACCESS GROUP MASTER LIST — SAMPLE REPORT

```
06/10/96                    HIGHLAND ELECTRONICS              Page  1
10:03                       Access Group Master List

Group Group Description                Code  Code Description                  SFS
_____ _____________________________    ____  ____________________________    ___

    1 DWNLD 801/802/8100/4222             5  DWNLD 801 ACCESS CODE            N
    1 DWNLD 801/802/8100/4222             6  DWNLD 802 ACCESS CODE            N

    2 SFS/708/801/802/8100/4222           1  HOST 422, 808 & 708              N
    2 SFS/708/801/802/8100/4222           3  DWNLD 804 ALPHA LAB 808S #2      N
    2 SFS/708/801/802/8100/4222           4  DWNLD 805 ALPHA LAB 808S #3      N
```

ACCESS OVERRIDE

The report lists access override codes in the database, with descriptions, start / end dates, and permissions (allow / deny access). A sample screen follows:

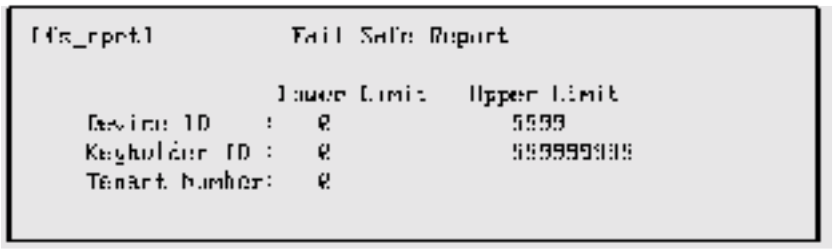


ACCESS OVERRIDE — SAMPLE REPORT

```
03/25/96                          Security Electronics          Page 1
08:21                             Access Override Codes

Code   Description                    Start      End        Permission
____   ____________________________   ________   ________   __________
  1    TEST OVERRIDE ALLOW            03/21/96   03/24/96   Allowed
  2    TOXIC CHEMICALS IN USE         04/14/96   04/14/96   Allowed
900    RDI OVERRIDE CODE              05/11/96   05/11/96   Denied
999    TEST OVERRIDE DENIED           05/25/96   05/26/96   Denied
```

INTELLIGENT FAIL SOFT REPORT

The intelligent fail soft report function, used in the event of a communications failure, lists keyholder access permissions for each 708P in the system . The report begins a new page for each device, and shows the readers attached to a device, and the keyholders and their access permissions by individual reader. Fail soft access is used only when a 708P cannot communicate with the host computer. A sample screen follows:



INTELLIGENT FAIL SOFT — SAMPLE REPORT

```
03/25/96                              Soames Industries                    Page  1
08:24                                 Intelligent Fail Soft Report

Keyholder   Keyholder Name            7110  7120  7130  7140  7150  7160  7170  7180
_________   ______________________    ____  ____  ____  ____  ____  ____  ____  ____

   67100    708P PARKING CNTR

   63455    DIGI FI-GI                Y     Y     Y     Y     Y     Y     Y     Y
   61096    GUARD NEW                 Y     Y     Y     Y     Y     Y     Y     Y
   61099    1030 ALT+D+P              Y     Y     Y     Y     Y     Y     Y     Y
```

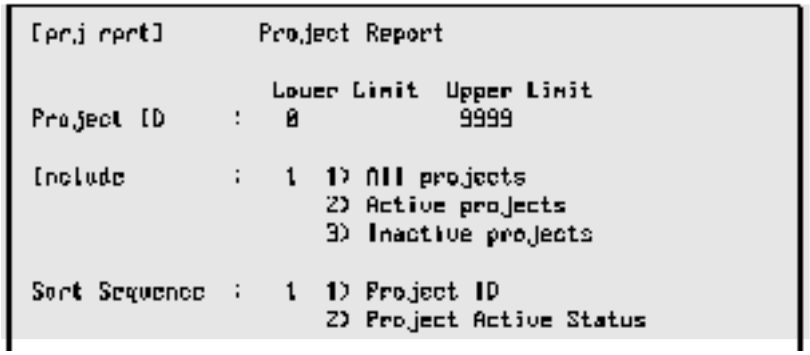
PROJECT REPORT

The Project Report includes number, description, start / stop times and dates, and current status.

NOTE

This report gives project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

A sample project report screen follows:



PROJECT REPORT — SAMPLE REPORT

```
03/25/96                                Security Electronics              Page   1
08:29                                   Project Report

Project  Project Description          S.Date    S.Time E.Date    E.Time Schedule
_______  ___________________________ ________  _______ ________  _______ ________

    1    TEST PROJECT #1              06/01/96  15:52  06/01/96  15:56  Active
    2    TEST PROJECT #2              06/05/96  07:30  06/06/96  23:59  Inactive
    5    EMERGENCY CIRCUITBOARD REV.  12/17/96  00:00  01/01/99  23:59  Active
   50    NEW TEST PROJECT             06/23/96  00:00  06/25/96  23:59  Inactive
   51    LAUNCH                       02/16/96  08:00  02/20/96  17:00  Inactive
  100    TEST PROJECT #3              06/05/96  00:00  06/10/96  23:59  Inactive
```

KEYHOLDER PROJECT REPORT

The Keyholder Project Report includes keyholder ID, name, project ID and description, and current status. A sample keyholder project report screen follows:

NOTE

This report gives keyholder project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

```
[epj rprt]       Keyholder / Project Report

                  Lower Limit  Upper Limit
Keyholder ID   :   0            999999999
Project ID     :   0            9999

Include        :   1  1) All projects
                      2) Active projects
                      3) Inactive projects

Sort Sequence  :   1  1) Keyholder ID
                      2) Project ID
                      3) Keyholder Name
```

KEYHOLDER PROJECT REPORT — SAMPLE REPORT

```
05/05/96                        Security Electronics              Page  1
13:47                           Keyholder / Project Report

Keyholder  Keyholder Name      Project   Project Description      Schedule
_________  ___________________ _______  ________________________ ________

   661091  BOB SMITH                 2   TEST PROJECT #2          Active

   661093  JOHN MILLAR               1   TEST PROJECT #1          Inactive
```

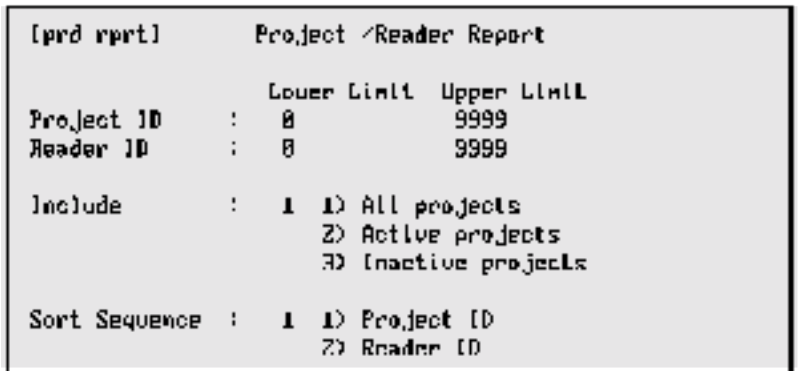
READER PROJECT REPORT

The Reader Project Report lists project number, description, readers assigned, current status.

NOTE

This report gives reader project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

A sample reader project report screen follows:

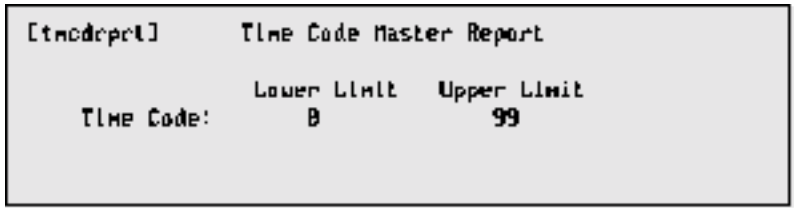


READER PROJECT REPORT — SAMPLE REPORT

```
05/05/96                              Security Electronics                    Page   1
13:42                                 Project / Reader Report

Project   Project Description                    Schedule   Reader   Reader Description
_______   ____________________________________   ________   ______   ________________________

10        TEST PROJECT #1                        Active     8110     808SX DOOR 1
                                                            8120     808SX DOOR 2

15        EMERG. CIRCUIT BOARD REV. PROJECT      Active     1001     422 ENTRY #1
                                                            1010     818 #7 DOOR #1 ALPHA
```

TIME CODES

This report lists all time codes set up in the database. A sample screen follows:

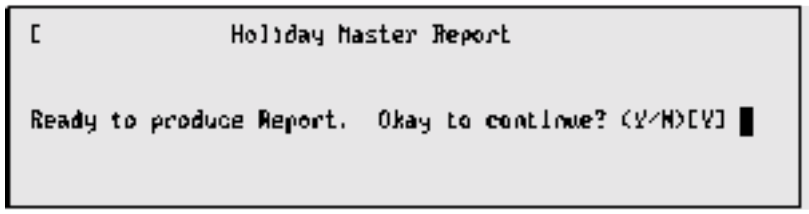


TIME CODES — SAMPLE REPORT

```
03/25/96                          Security Electronics          Page 1
08:36                             Timecode Report

Tmcd  Description                 Start  End    Mon Tue Wed Thu Fri Sat Sun Hol
____  ____________________________ _____ _____  ___ ___ ___ ___ ___ ___ ___ ___

  0   NEVER ACTIVE                00:00  00:00  N   N   N   N   N   N   N   N
  1   7-DAYS, 24-HOURS & HOLS     00:00  23:59  Y   Y   Y   Y   Y   Y   Y   Y
  2   OFFICE HOURS 7 am - 6 pm    07:00  18:00  Y   Y   Y   Y   Y   N   N   N
  3   WEEKENDS & HOLIDAYS         00:00  23:59  N   N   N   N   N   Y   Y   Y
```

HOLIDAYS

This report lists all holidays that have been entered into the system. A sample screen follows:

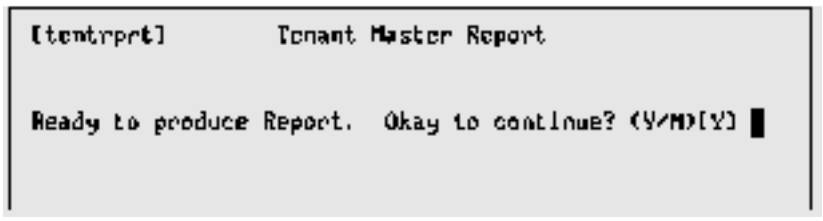


HOLIDAY CODES — SAMPLE REPORT

```
 03/25/96                          Jamestown Aircraft                Page 1
 08:38                             Holiday Master Report

 Date       Description
 ________   ____________________________

01/01/96    NEW YEAR'S DAY
05/27/96    MEMORIAL DAY
07/04/96    INDEPENDENCE DAY
09/01/96    LABOR DAY
11/28/96    THANKSGIVING DAY
11/29/96    DAY AFTER THANKSGIVING
12/24/96    CHRISTMAS EVE
12/25/96    CHRISTMAS DAY
```

TENANTS

This report lists all tenant names and numbers defined in the system. A sample screen follows:

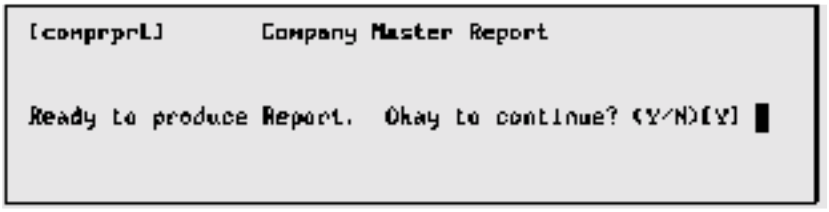


TENANTS — SAMPLE REPORT

```
05/04/96                          TRADE CENTER MAIN            Page  1
09:07                             Tenant Report

Number  Description
______  ___________
     1  WESTWOOD SECURITY SYSTEMS
     2  SOS PUBLISHING (CALIFORNIA)
     3  BETA SOFTWARE
     4  WALKINS PRODUCTS, INC
```

COMPANY, DEPT, LOCATION, JOB CAT

These reports list user-defined company, department, location and job category information. The report screens are identical for all four — a sample follows:

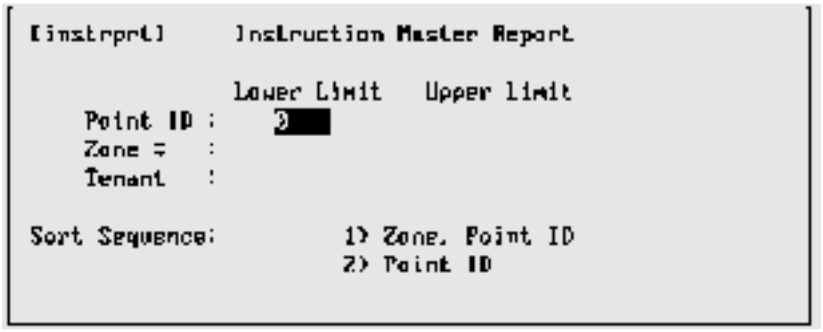


COMPANY, DEPT, LOCATION, JOB CAT — SAMPLE COMPANY REPORT

```
03/25/96                          Security Electronics             Page  1
08:41                             Company Master List

           Number      Description
           ______      ____________________________

                1      DRAYTON ENGINEERING
                2      SMITH-JONES WAFER FAB.
                3      MCDOWELL PUBLICATIONS
```

INSTRUCTIONS

This report lists the operator instructions to be taken following specified events occurring at specified points. A sample screen follows:



SAMPLE INSTRUCTIONS

```
03/25/96                          General Electronics Co                Page  1
08:45                             Instruction Master List

Point  Point Description               Zone  Instructions
_____  ___________________________________  ____  ____________________________________________

 7114  PRIORITY 10 ALARM                    4  EVACUATE LAB AREA
                                              NOTIFY BUILDING MANAGER PAGER #12345
                                              DIRECT FIRE CREW TO SCENE
                                              PROVIDE ASSISTANCE AS NECESSARY
                                              LOG EVENT START/STOP IN SHIFT LOG



 9011  RDI 808 #1 1.1 FIRE                   5  REMOTE SITE FIRE ALARM
                                              CALL 777-1212 AND NOTIFY LOCAL FIRE DEPT
                                              NOTIFY OPERATIONS MANAGER PAGER #12345
                                              LOG EVENT IN SHIFT LOG BOOK
```

MAPS

The map report lists all points incorporated into user-defined system maps. The report screen prompts only for the desired sequence: point ID, point type, or map name.

SAMPLE REPORT — MAP INFORMATION

```
03/25/96                              CAMPBELL TECHNOLOGY                Page  1
09:33                                 Map Definition Report

 Point   Point Type   Map Name
 _____   __________   ____________________________

     1   CAMERA       HLP_PNTS
     1   DOOR         HLP_DOOR
     2   DOOR         HLP_DOOR
     2   SENSOR       HLP_PNTS
     3   ALARM        HLP_PNTS
```

DEVICE CONFIGURATION REPORTS

ZONES

This report lists all zones defined in the system. A sample screen follows:

```
[zonerprt]        Zone Master Report

Ready to produce Report  Okay to continue? (Y/N)[Y] _
```

ZONES — SAMPLE REPORT

```
03/25/96                          Leigh-Haffner Enterprises       Page  1
08:47                             Zone Report

 Zone  Description                        Area  Prim  Level
 ____  ___________________________________  ____  ____  _____

    1  ALPHA LAB ZONE                     P     H     G
    2  HARD PASSBACK ZONE 2               P     H     L
    3  HARD PASSBACK ZONE 3               P     H     L
    4  HARD ANTI PASSBACK                 V     H     G
```

POLLERS

The report lists all defined pollers in the system. A sample screen follows:

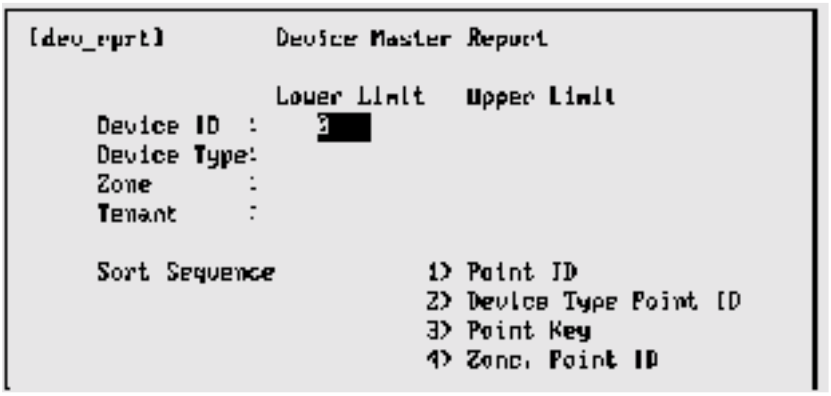
```
[pol_rprL]        Poller Master Report

                  Lower Limit   Upper Limit
     Point ID   :    3
     Poller Type:
     Zone       :
     Tenant     :

     Sort Sequence          1) Point ID
                            2) Point Type, Point ID
                            3) Point Key
                            4) Zone, Point ID
```

POLLERS — SAMPLE REPORT

```
03/25/96                          Global Software                 Page  1
08:49                             Poller Master Report

 Poller  Date In                Comp #  Poll # Prim  Poller Type Desc  Disabled Zone  Zone Desc
 ______  ______________________ ______  ______ ____  _________________ ________ ____  _________

      2  DATABASE POLLER        0       0      11    Database          NO          0  OUTSIDE
      3  422/808 POLLER 1       0       1      6     808               YES         0  OUTSIDE
      4  808/422 POLLER 2       0       2      6     808               NO          0  OUTSIDE
      5  708P PARK POLLER 5     0       5      8     Parking           NO          0  OUTSIDE
```

DEVICES

This report lists all devices defined in the system. A sample screen follows:

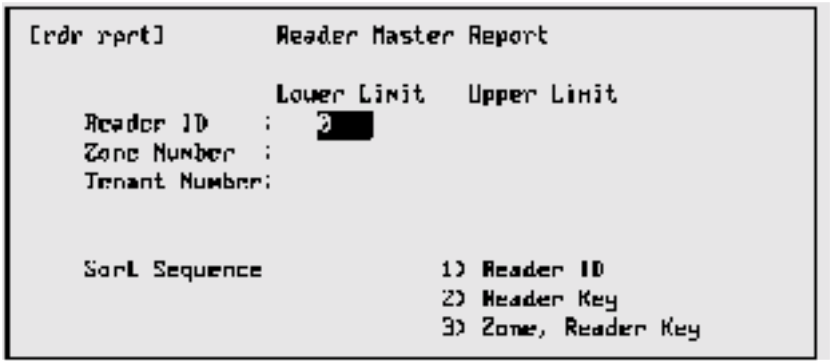


DEVICES — SAMPLE REPORT

```
03/25/96                                McCartney Foundation                    Page  1
08:50                                   Device Master Report

 Device  Device Desc          Comp #Poll #  Address  Prim Device Type Desc  Disabled   Zone Zone Description
_____________________________________________________________________________________________________

      1  HOST                   0    0        0        1  Host              NO         0    OUTSIDE
     10  LC #1                  1    0        0        2  Controller        NO         0    OUTSIDE BUILDING
    100  DIAL-UP 422 #1       100    0        1       15  SE422             YES        0    OUTSIDE BUILDING
    801  BETA 808 SX# 2         0    2        2       10  808SX/SN          NO         2    HARD PASS BACK ZONE 2
    802  BETA 804S #1           0    2        1        4  808S              NO         2    HARD PASS BACK ZONE 2
```

READERS

This report lists all readers defined in the system. A sample screen follows:



READERS — SAMPLE REPORT

```
06/03/96                                LOVELL-WATKINS INC.                          Page   1
12:57                                   Reader Master Report

Reader Reader Description   Comp #   Poll Dev   Sen   Point Type  Zone   Dir   Disd  Dsid Desc   Rex  Rex Desc
______ ____________________ ______   ____ ___   ___   __________ ____   ___   ____  _________   ___  ________

295    RM-A EAST ENTRY       1      16     1      1  Acc Ctrl     1    N/A   2241  2240
                                                Tmcd   Start   End     Mon   Tue  Wed  Thu   Fri   Sat   Sun   Hol
                                                ____   _____   _____   ___   ___  ___  ___   ___   ___   ___   ___
                                                1      00:00   23:59   Y     Y    Y    Y     Y     Y     Y     Y

296    RM-A WEST ENTRY       1      16     1      2  Acc Ctrl     1    N/A   2245  2244
                                                Tmcd   Start   End     Mon   Tue  Wed  Thu   Fri   Sat   Sun   Hol
                                                ____   _____   _____   ___   ___  ___  ___   ___   ___   ___   ___
                                                1      00:00   23:59   Y     Y    Y    Y     Y     Y     Y     Y
```

POINTS

This report lists all points defined in the system. A sample screen follows:

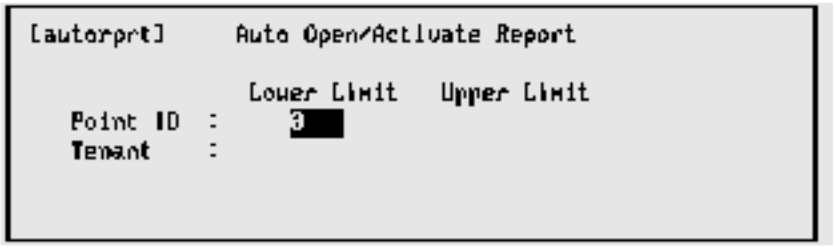
```
[pnt rprt]          Point Master Report

                    Lower Limit   Upper Limit
     Point ID  :       1
     Point Type:
     Zone      :
     Tenant    :

     Sort Sequence:          1) Point Id
                             2) Point Type, Point Id
                             3) Point Key
                             4) Zone, Point Id
```

POINTS — SAMPLE REPORT

```
07/16/96                                Datastyles, Inc                              Page 1
11:51                                   Point Master List

Point Point Description    Comp# Pol   Dev  Sen Con  Point Type  Zone Trace  I/O  Enable   Normal
_____ ___________________ _____ ____  ___  ___ ___  __________ ____ _____  ___  _______  ______
  93  LOT 1 (IN) DS       0     1     1    1   1    Door Switch 0    NO     IN            OPEN

                                                  Tmcd Start      End     Mon Tue Wed Thu Fri Sat Sun Hol
                                                  ____ _____      _____   ___ ___ ___ ___ ___ ___ ___ ___
                                                  2    17:00      06:00   Y   Y   Y   Y   Y   Y   Y   Y

  94  LOT 1 (IN) RX       0     1     1    1   2    Open on Rex 0    NO     IN            OPEN

                                                  Tmcd Start      End     Mon Tue Wed Thu Fri Sat Sun Hol
                                                  ____ _____      _____   ___ ___ ___ ___ ___ ___ ___ ___
                                                  1    00:00      23:59   Y   Y   Y   Y   Y   Y   Y   Y
```

AUTO OPENS / ACTIVATES

This report lists system points and readers which have auto-open or auto-activate times. A sample screen follows:

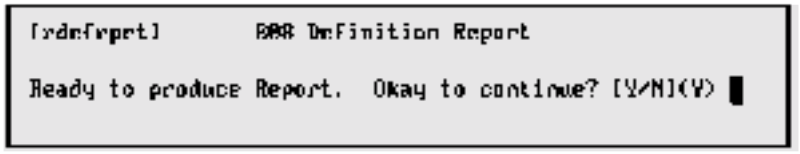


AUTO OPEN / ACTIVATE — SAMPLE REPORT

```
03/25/96                              Security Electronics                                    Page  1
08:54                              Auto Open/Activate Master List

Point  Point Description           Point Type  Tmcd  Start  End    Mon  Tue  Wed  Thu  Fri  Sat  Sun  Hol
_____  _____________________       __________  ____  _____  _____  ___  ___  ___  ___  ___  ___  ___  ___
1830   818 #7 DOOR #3 +VIP         READER        9   10:35  10:40  Y    Y    Y    Y    Y    N    N    N
1850   818 #7 DOOR #5              READER       14   11:29  12:31  Y    Y    Y    Y    Y    N    N    N
1870   818 #7 DOOR #7              READER       16   11:59  13:01  Y    Y    Y    Y    Y    N    N    N
8240   TIM'S 804S DOOR 4           READER        6   15:39  15:39  Y    Y    Y    Y    Y    N    N    N
```

808 REPORT DEFINITION

This report lists all action reports defined for the system 800-series ACUs. A sample screen follows:

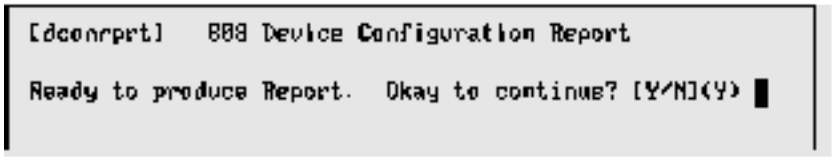


808 REPORT DEFINITION —SAMPLE REPORT

```
03/05/96                          Security Electronics                          Page   1
15:22                             808 Report Definition

 100      DIAL-UP 808 #1                    Report    1

                        Send To Host      Close Latch        Close Output
Bldg Open               Y                 N                  Y
Bldg Limited            Y                 N                  Y
Bldg Closed             Y                 N                  Y
Time Code               1                                    1
Time Code
Time Code
Contact Number
Print Asterisk With Log    N              Prevent Building Closure   N
```

808 DEVICE CONFIGURATION

This report lists configuration information for the system 800-series ACUs. A sample screen follows:



808 DEVICE CONFIGURATION — SAMPLE REPORT

```
06/05/96                          Simms Oil Corporation
15:25                             808 Device Configuration

 100  DIAL-UP 808 #1

Level Name          Password          Reports          Key Definition

A     OPERATOR MGR  NEW               Tamper       9   Primary Key Type     1060
A     G. SAYLES     SAYLSG            Power Fail   4   Aux. Key Type        NONE
B     LYNN VAUGHAN  LYNSID            Override     1   Facil Code           *
C     TIM JONES     TJO123            Alt Facil Code       A000
```

DIALERS

The two dialer report types detail the remote dialup interface (RDI) devices defined for the system or those RDI devices which have experienced communication trouble. A sample screen follows:

DIALERS — SAMPLE REPORT

```
03/25/96                              Security Electronics                  Page       1
09:00                                 Dial Master Report

Device   Device Description   Remote Number   Last Date   Last Time   Who Called  # Trans  # Failures
______   __________________   _____________   _________   _________   __________  _______  __________

  900    RDI - ALPHA LAB          4921342     02/19/94    17:10       Host            0          1
```

SITE DEFINITION

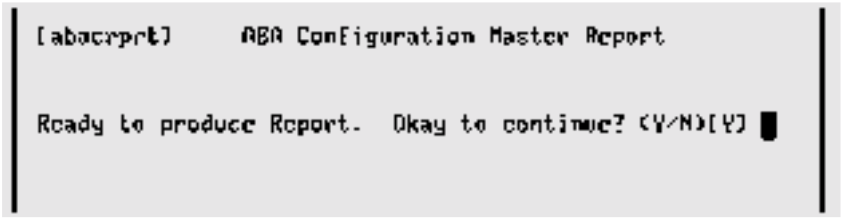
This report lists all site groups and codes defined for the system. A sample screen follows:

SITE DEFINITION — SAMPLE REPORT

```
03/25/96                          Security Electronics                Page  1
09:02                             Site Code Master Report

Group      Code
_____      ____

    1      0000
  100      1000
  101      1001
 6016      7279
```

ABA CONFIGURATION

This report lists all the ABA configurations defined for the system, and gives the configuration parameters. A sample screen follows:

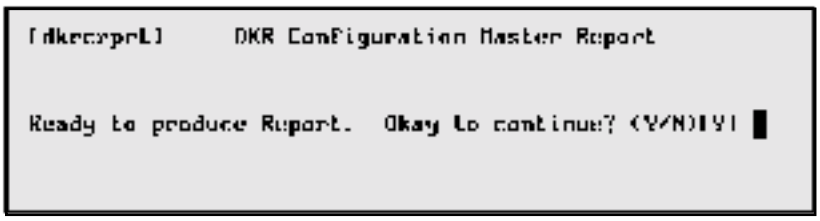


ABA CONFIGURATION — SAMPLE REPORT

```
03/25/96                            Security Electronics                          Page  1
09:17                             ABA Configuration Report

Configuration ID      1000
                     Start   Length
Key   A               1       3
Key   B               4       2
Key   C              10       3
Expiration Date Start          15     Site Code Start                20
ABA Key Data Action             0
                                                                     During Fail Soft
                                  Deny Access                        Deny Access
Based on key number               N                                  N
Based on site code                N                                  N
Based on expiration date          N                                  N
Use site code as key              N                                  N
```

DKR CONFIGURATION

The reports lists the system default DKR parameters. A sample screen follows:

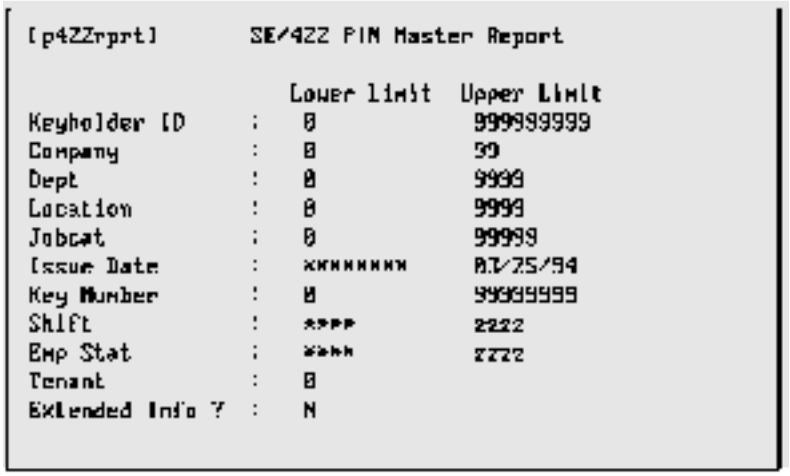


DKR CONFIGURATION — SAMPLE REPORT

```
06/12/96                                Lotus Refineries                          Page 1
15:21                                   DKR Configuration Report

                                                                Beeper Times    Red LED Times  Green LED Times
Config. ID  Send Once  Read Range Number of Reads  Read Time   On Off Total     On  Off Total    On  Off Total
     1          Y         255             1           100      20  30  20       0    0    0     0    0  0
```

SE 422 PIN MASTER REPORT

This report lists keyholders having system-calculated SE 422 PIN numbers. A sample screen follows:



SE 422 PIN MASTER REPORT — SAMPLE

```
03/25/96                              Soames Industries                          Page 1
09:22                                 SE/422 Quick List

Keyholder    Key No   Keyholder Name           Dept   Jobcat  Phone        Title       Loca Floor     422Pin
__________  _______  _____________________  _____  _______  ___________  __________  _____________  _______

      6109  1895573  Duane Eddie              1       3                  Assembler   Main Mfg Flr   60030
      6110  1784422  Juarez Sandi             1       3                  Assembler   Main Mfg Flr   31949
      6112  1901112  De Witt Charles          1       3                  Assembler   Main Mfg Flr   32112
      6113  1788122  Ames Linda               1       3                  Assembler   Main Mfg Flr   35976
```

132-COLUMN REPORT DISPLAY

The local print program was originally written to accommodate an 80-character terminal display. Some terminals now use up to 132 characters, and the new *132-Column Report Display* feature allows for this. The terminals are: HP700/44; HP700/92; Color PC terminals using *Reflections 4* terminal emulation software. The feature is automatically enabled, and automatically resumes the 80-character display mode when the user exits the report program. A sample 132-character display follows:

NOTE

1. When in the 132-column mode, the terminal scrolls one half page at a time.

2. This new feature is not supported by the HP console terminal provided with the host and LC systems.

132-COLUMN REPORT — SAMPLE DISPLAY

```
Point  Point Description   Zone  Date      Time      Access Type                  Keyholder  Keyholder Name     Key No
_____  ___________________ ____  ________  ________  ___________________________  _________  _______________   _______

8110   TIM's 808SX DOOR 1   801  11/18/96 07:28:26  PROJECT ACCESS GRANTED       123456789  TIM H+P+SMF       5825175
8110   TIM's 808SX DOOR 1   801  11/18/96 07:28:06  INVALID PROJECT              123456789  TIM H+P+SMF       5825175
8110   TIM's 808SX DOOR 1   801  11/16/96 08:32:58  PROJECT ACCESS GRANTED       123456789  TIM H+P+SMF       5825175
8110   TIM's 808SX DOOR 1   801  11/16/96 08:22:10  PROJECT ACCESS GRANTED       123456789  TIM H+P+SMF       5825175
```

SECTION 6
SYSTEM ADMINISTRATION

INTRODUCTION

The administration functions are used to control and maintain the system. These functions are accessed from the system administration menu, [sys_menu], via the main menu. (Depending on the operator's program security level, some or all of these functions may not be available.) A sample screen follows:

SECTION ORGANIZATION

The procedures in this section are in the order shown in the system administration menu (above). The associated subscreens also follow in order. After the current screen has been saved, most subscreens display by pressing F2 but some display automatically.

ADDITIONAL INFORMATION

Additional system administration-related information is provided at the conclusion of this section.

ADD USERS [addusers]

The add users screen, [addusers], is entered to add, change, or delete system users / operators.

IMPORTANT

The administration log-on and password must be used to access this screen. If you are already logged on with your regular password, first log off in the normal way, then log on again using the administration log-on and password.

A sample [addusers] screen follows:

User Name. Required. Enter the user name (first eight letters of last name recommended).

Keyholder ID. Optional. User's keyholder ID. Default is 0. You should have a keyholders ID assigned to you. When you enter this menu, your name is displayed at the top of the screen.

3 **Program Security Level**. Optional (range 1—9999). Code number indicating the specific screens the user can access. Default is 1 (complete access).

4 **Tenant**. Optional. Enter tenant number (if applicable). Default is tenant 0.

5 **Monitoring Group**. Optional. System code indicating transaction types available to this user. Default is * — All transaction types.

Transactions may be defined as elements of monitoring groups. For example, access granted transactions could be placed in monitoring group A, door forced open transactions could be placed in monitoring group B, all other transactions could be placed in monitoring group 0 (zero)—the field default. Assignments for these groups could be:

Group A — Assigned to those who need only to monitor day-to-day access granted transactions.

Group B — Assigned to security guards who need to see all door forced open transactions.

Group 0 — Assigned to the system administrator who needs to see all transactions.

6 **Monitoring Security Level**. System code (0, 1, or 2) indicating the user's monitoring / data changing capabilities. Monitoring security level 0 allows full monitoring / changing capabilities, including disabling points and halting pollers. Monitoring security level 1 is recommended for general use, since it permits a user to control certain functions, such as doors, but not pollers and points. Monitoring security level 2 limits users to a purely observational capacity; no functions can be controlled.

IMPORTANT

1. We recommend that level 0 be assigned only to completely trained and responsible personnel, since some level 0 operations could easily disable the system if not performed correctly.

2. Enter **C** in this field to use the new enhanced security monitoring feature (see *Enhanced Monitor Security* below).

7 **Allow Alarm Servicing**. **Y** / **N** / **F** field indicating if the user has the authority to respond to alarms in the monitor program, or enter **F** if the alarm fast acknowledgment feature is to be allowed.

8 **Jump Alarm Servicing**. **Y** / **N** field indicating if the user has the authority to automatically jump to alarm servicing from monitor when an alarm occurs.

9. **Jump Timer Servicing**. **Y** / **N** field indicating if the user has the authority to automatically jump to timer servicing from monitor when an timer event occurs.

10. **Language**. The code number entered will determine what language the system will use for this user. Valid choices are 1=English, 2=French.

11. **Real-Time Maps Security Level**. 0=Complete functionality, 2=View maps only (no control capabilities).

MODIFY PASSWORDS [mod_pass]

Use the modify password screen to change an existing password (must be logged in as *addusers*). Enter the user name, then follow screen prompts. A sample screen follows:

```
[mod_pass]                  Modify Passwords


Enter User Name or press ENTER to exit:  tim
Setting password for user: tim
Last   successful password change for tim: Mon Oct 16 13:53:20 1995

                Choose password

You can choose whether you pick a password,
or have the system create one for you.

        1. Pick a password
        2. Pronounceable password will be generated for you

Enter choice (default is 1):
```

Enter the password twice to confirm it.

NOTE

If you enter a user name but then decide that the password does not need to be changed, then the current password must be reentered.

To return to the system administration menu after the new password has been entered, first press **Enter** to return to

```
[mod_pass]                  Modify Passwords


Enter User Name or press ENTER to exit:
```

then press **Enter** again.

PROGRAM SECURITY [sec_menu]

PROGRAM SECURITY LEVEL ENTRY [pgacentr]

Begin creating program security level types by first displaying the program security level entry screen [pgacentr]:

1. Enter the security level number (four digits maximum).

2. Enter a description (30 characters maximum).

Press F6 Store, then press F2 for the program security level definition screen

PROGRAM SECURITY ENTRY DEFINITION [pg1_entr]

Press F7; the first six system data items display:

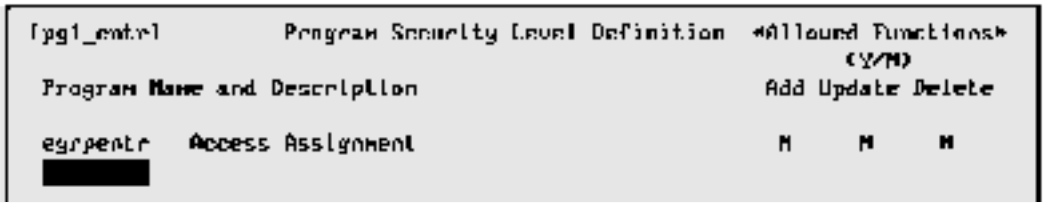
Arrow down to the first system item for this new security level; press F1. The system displays the program name and description to the left, and the add/update/delete fields to the right. For example:

Enter Y or N in the add/update/delete fields to give or deny access to these functions on the selected screen. If you do not make any Y/N selection in the Add, Update, and delete fields, the keyholder will not have access to the screen. Press F6 Store and then, before any other action is taken, press F5 to return to the add mode for the next entry. Repeat these actions for all items in the new security level. Note that the Add, Update, Delete fields only apply to screens with this capability not to menus.

NOTE

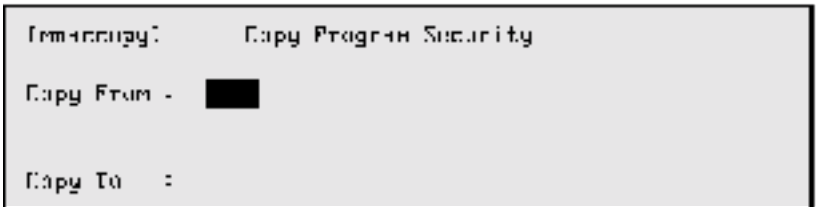
1. Add items to an existing program security using the foregoing methods.

2. To delete an item, first select as shown above then use Esc, d, r.



COPY SECURITY [mnaccopy]

It may be easier to copy an existing security level and make changes to this when creating a new security level. To do this, display the [mnaccopy] (Copy Program Security) screen, enter the existing security level number in the Copy From field and enter the new security level number and description in the Copy To field. Make changes to the new security level using the above procedures.



SECURITY MASTER LIST [pgacrprt]

Use the security master list [pgacrprt] facility to print a listing of all security levels established for your system or those for a selected range. A complete list is given in *Appendix D: Program Security Master List*.

DISPLAY ALL VALID LOGINS [showuser]

Use the [showuser] screen to identify — by hard copy printout or report display at the system terminal — all operators who have access to the system (use the [showwho] (Display All Valid Logins) screen to display operators currently logged on. Follow prompts when the screen displays. A sample report is recreated below:

```
10/23/96                Eton Engineering              Page 1
13:02

Login Name           Tenant   Security   Keyholder
___________________  ______   ________   _________
anderson             0        1            1123456
melville             0        1            1334229
smith                0        1            1348876
```

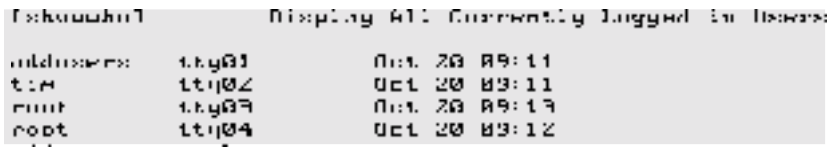
DISPLAY CURRENT DATE AND TIME [showdate]

Use the [showdate] screen to display the current system date and time. A sample display follows:

```
[showdate]              Display Current System Date

Fri Oct 20 09:14:00 PDT 1995
Press RETURN to continue.
```

DISPLAY ALL USERS WHO ARE LOGGED IN [showwho]

Use the [showwho] screen to display operators currently logged in (use the [showuser] screen to identify all operators who have access to the system). Follow prompts when the screen displays. A sample report is recreated below:

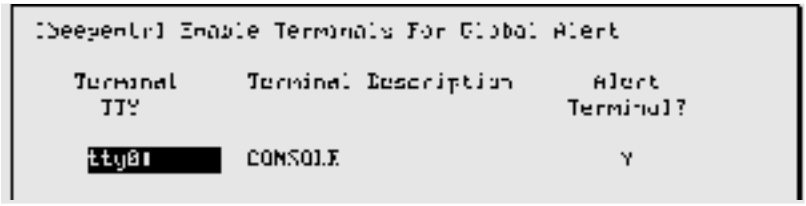


PURGE A PENDING REPORT [purgrprt]

Use this feature to halt a report currently being printed (applies only to reports created under your ID). The feature can also be used to display reports. Note that if you log on using addusers you will have complete printer control.

ENABLE TERMINALS FOR GLOBAL BEEPING [beepentr]

This feature is used to enable terminals to beep when an alarm occurs. Obtain terminal IDs (port connection — *tty___)* from system installer and enter with optional description.

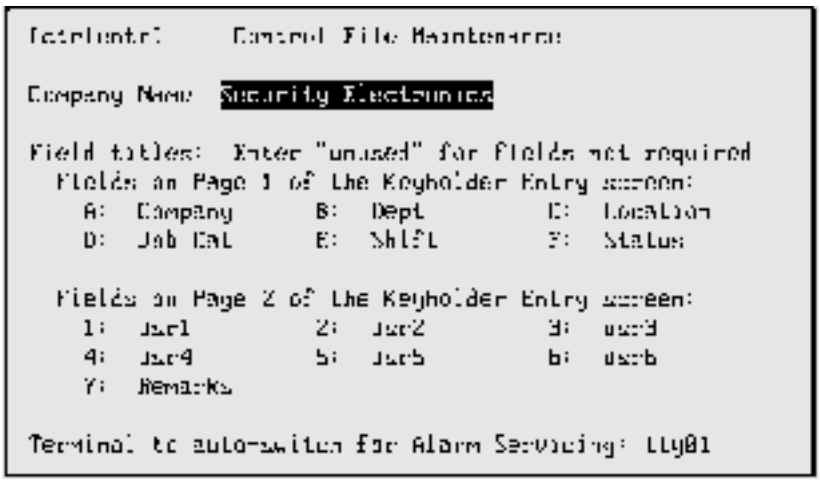


SYSTEM CONFIGURATION (syclmenu)

CONTROL FILE MAINTENANCE [ctrlentr]

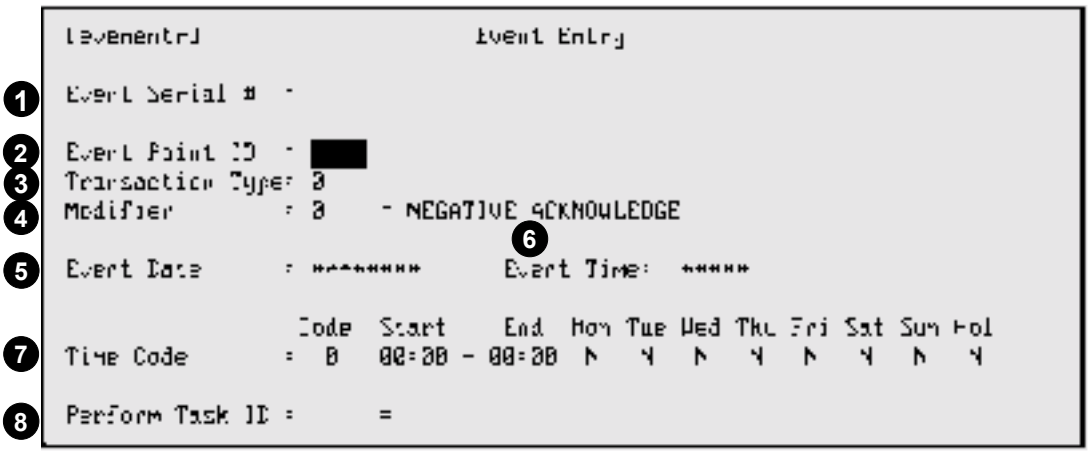
For informational / custom reporting purposes, certain field titles that display in keyholder record screens [key_entr] and [key1entr] can be changed to suit the individual user. Since keyholder records may be considered the primary data items for an access control system, many SE 6000 owners use the field title change feature to tailor the system to their precise requirements. Change fields A through F and 1 through 7 as required.

TERMINAL AUTO SWITCH [ctrlentr]. An additional field at the foot of this screen is optionally used to set up a particular terminal to automatically switch to the alarm servicing screen (from monitor) when an alarm occurs. A sample screen follows:



EVENTS [evenentr]

The task / event subsystem is used to program one or more tasks to be automatically performed in response to the occurrence of a user-defined event. Tasks and events are linked, and the task must be entered and stored before the system allows the creation of a related event. Events can initiate the same task, or a single event can initiate multiple tasks. Events controlled by a time code automatically perform the task entered in the activate field at the start of the code and the task entered under the deactivate code at the end of the time code. A sample screen follows:



Event Serial #. System-assigned. Keeps track of all event entries.

Event Point ID. Required. The point ID at which a specified transaction must occur to initiate a task (can be time code or event date initiated).

Transaction Type. Required. The transaction number which must occur at the specified point ID to generate a task (see *Appendix C: System Transactions* for a list of the system-generated transactions numbers).

Modifier. Optional. If applicable, the transaction modifier which defines the event if the message is user-defined.

Event Date. Optional. If the task referenced by this event is to be system-initiated, enter the applicable date.

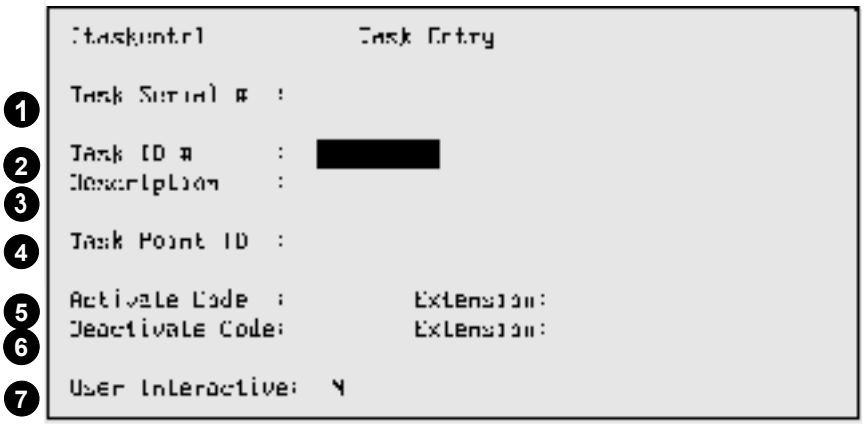
Event Time. Optional. If the task referenced by this event is to be system-initiated, enter the applicable time.

Time Code. Optional. If the task referenced by this event applies to a specific time code, enter the time code number.

Perform Task ID. Required. Enter the task ID number.

TASKS [taskentr]

Used to set up tasks for the task / event subsystem. Tasks must be created before the associated event.



Task Serial #. System-assigned number used to keep track of all tasks.

Task ID. Required. Enter a user-assigned task ID number. Task IDs do not have to be unique. All occurrences of a given task will be executed by an associated event.

Description. Optional. Enter a brief description of the task.

Task Point ID. Required. Point ID number controlled by this task.

Activate Code, **Extension**. Required. System code number for the type of action to be performed. The extension applies to camera presets for pan and tilt, or image verification when used with a Polaroid ID-4000 system. See table following this field description list.

Deactivate Code, **Extension**. Optional. If this task is to be automatically controlled by a time coded event, enter the activate / deactivate code to be executed when the event time code ends. See table following this field description list.

User Interactive. Conditional (applies to event times). A Y/N field to indicate if a timed task can be cancelled by an operator.

ACTIVATE / DEACTIVATE CODES

09	REQ MANUAL ACCESS	Request to perform manual access.
29	FORGIVE PASSBACK	Request to forgive passback.
41	MANUAL UNLOCK	Unlock a sensor / lock for an unlimited time.
45	MANUAL LOCK	Lock a sensor /lock.
46	TIME UNLOCK	Unlock a sensor / lock for the amount of time specified by the hardware settings, or, where applicable, by the amount of time in the *Unlock Time* field of the reader entry screen.
56	BUILDING OPEN	Set building mode to OPEN
57	BUILDING LIMITED	Set building mode to LIMITED
58	BUILDING CLOSED	Set building mode to CLOSED
70	DEACTIVATE OUTPUT	Turn off the specified output. Use this code if you are elsewhere turning an output on for an unlimited time.
71	ACTIVATE OUTPUT	Turn on a specified output for the amount of time shown in the *Time* field on the point entry screen. If *Time*=0, the output will be on for an unlimited amount of time, and you must turn it off with an a deactivate output code.
80	Chain Task	Jumps to another group of task records and is used to consolidate multiple task into a separate task.
81	EXTENDED PROCESSING	Instruct extended processing poller to process a transaction. Use with elevator, parking control, VIP2, and poller transactions with a point ID which matches the poller record for these functions.
89	SHUNT POINT	Shunt a specified point.
90	UNSHUNT POINT	Unshunt a specified point.
91	REQUEST RESET DEVICE	Perform a device reset for an applicable device.
92	REQUEST RESET KEYS	Perform a key download for an applicable device.

100	ACTIVATE PROJECT	Activate an inactive project.
101	DEACTIVATE PROJECT	Deactivate an active project.
102	NORMALIZE or CLEAR PROJECT	Change project status to its normal condition (clears an override condition).

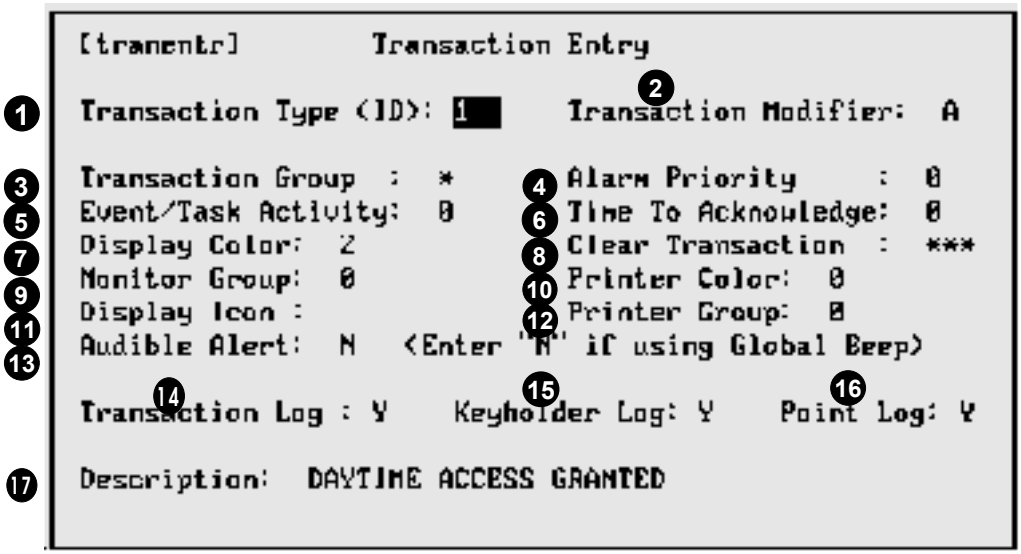
TASK EVENT / MASTER REPORT [taskrprt]

This report shows all tasks / events established in the system:

```
04/14/96                          ATARAXIA ELECTRONICS                              Page 1
13:02

 Task  Task Description            Point      Activate Desc       Deactivate Desc      Cancelable
_____  _____________________       _______    _______________     _________________    __________
   42  UNLOCK DOOR                 708 #2     ENTER ZONE B        Man Open                       N

EVENTS                            7120   708 #2 ENTER ZONE B        62 0 KEY NOT ACTIVE  No Activity
                                           Tmcd   Start   End     Mon  Tue  Wed  Thu  Fri  Sat  Sun  Hol
                                           ____   _____   _____   ___  ___  ___  ___  ___  ___  ___  ___
                                             1    15:30   16:15   Y    Y    Y    Y    Y    N    N    N
```

TRANSACTIONS [tranentr]

Customized versions of any system transaction (log message) can be created. The custom transactions are created using the transaction entry screen, where they are linked to the point or reader screens by a transaction modifier code. The codes are any of the following: A — Z (uppercase), a — z (lowercase), 1 — 9 (0 is the default modifier for all standard transactions). (Up to 62 log messages can be associated with the same event.)



Transaction Type (ID). The unique ID number of a transaction. The system is pre-programmed to use specific transaction types for certain events at certain types of points. (See *Appendix C: System Transactions* for a complete list of standard transactions.)

Transaction Modifier. Required as applicable. Enter a transaction modifier code to indicate a customized version of a standard transaction. The values are: A through Z (all uppercase), a through z (all lowercase), 0 through 9.

Transaction Group. For future use. Will permit the categorizing of transactions into broader groups for easier reporting and editing.

Alarm Priority. Conditional. Used to declare that a particular transaction is an alarm transaction, and to indicate the alarm priority. The range is 1 through 9, with 1 being the highest priority and 9 the lowest. Enter 0 for a non-alarm transaction.

Event/Task Activity. Conditional. Used if the system has been programmed to respond to a particular event via the event / task subsystem. Enter 1 to activate the task; enter 2 to deactivate the task.

Time to Acknowledge. Enter a value in minutes to allow for alarm acknowledgment. If the alarm is not acknowledged by this time, an ALARM NOT ACKNOWLEDGED message is written to the log and repeats at the interval specified until acknowledged.

Display Color. Determines the transaction display color in the monitor mode. The colors are:

0 = Black
1 = Red
2 = Green
3 = Cyan (light blue)
4 = Blue

Clear Transaction. Conditional. Enter the alarm clearing transaction number. For example, with transaction 92 (Alarm Active), enter 93 (Alarm Clear) as the clearing transaction. If a clearing transaction is specified, the alarm event cannot be removed from the pending alarms screen until the clearing transaction is received.

Monitor Group. Used to classify transactions into groups, so that the display of transactions based on log-in name can be controlled. The default monitor group assignment when users are added to the system is * — All monitor groups displayed.

Printer Color. Determines the color in which this transaction will display when printed on a color-capable log printer. The colors are:

0 = Black
1 = Red

2 = Green
3 = Cyan (light blue)
4 = Blue

Display Icon. For future use.

Printer Group. Each log printer must include the selected printer group in its list of available printer groups. If the selected printer group is not included, the transaction will not be printed on the log printer. Printers are preset to include all transactions (Printer Group=*). To prevent a transaction from printing, assign it to a printer group other than 0, then change the printer to 0.

Audible Alert. Indicates with **N** (none), **S** (single), or **C** (continuous) the type of audible alert which this transaction should produce (applies only if a user is in the monitor mode). If you wish to have a terminal alerted whenever this transaction occurs, enter **N** in this field.

Transaction Log. **Y / N** field to indicate if this transaction is to be stored in the archive history file on disk. The transaction history file is listed using the transaction history report.

Keyholder Log. **Y / N** field to indicate if this transaction is to be stored in the keyholder history file on disk. The system keeps a small area of disk space available to store the last 20 events for all individual keyholders in the system. The keyholder history file is listed using the keyholder history report.

Point Log. **Y / N** field to indicate if this transaction is to be stored in the point history file on disk. The system keeps a small area of disk space available to store the last 20 events for all individual points in the system. The point history file is listed using the point history report.

Description. Used to define the transaction description displayed on the monitor screen.

DATABASE MAINTENANCE [db_menu]

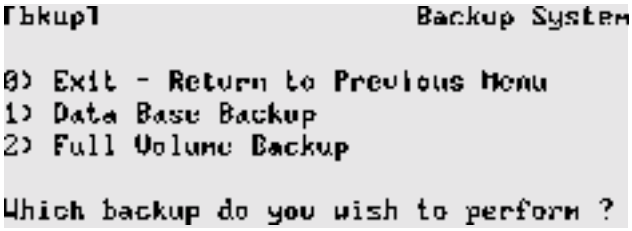
DISPLAY DATABASE STATISTICS [dbstats]

Display this data regularly to control disk space usage. Note the PUBLIC.archist table size near the end of the report. The table size indicates the number of transactions currently stored. Perform an archive whenever the row count is roughly 80% of the expected number of rows.

A message is displayed if the row count reaches the expected number of rows. If this happens, archive immediately. Two other tables should be checked regularly and purged if the expected number of rows exceeds 80%: PUBLIC.download; PUBLIC.alrmtran.

PERFORM BACKUP [bkup]

Two backup types are available — Database and Full Volume:



DATABASE BACKUP. A database backup copies all information in the database (exceptions user and map information). If you make a number of changes to keyholder, hardware, and / or access information in a single day, then the database backup should be performed each day. For these purposes, use two alternating tapes (one for odd days, one for even) to guarantee that no information will be lost in the event of a hardware malfunction.

FULL VOLUME BACKUP. A full volume backup copies all system data including programs, system configuration information, and user / map information. The backup tape created is used to restore the system in the event of a hardware malfunction. A full volume backup should be performed immediately following system installation, and then on a monthly basis or whenever there has been a major system update or reconfiguration.

DOWNLOAD CLEAN UP AND RETRY [downcln]

Download records are data transferred from the database to computer memory or to intelligent remote devices. Each time information is entered and stored in the database, one or more download records are created and written to the download file. If the download transfers are unsuccessful, the number of records created can increase the download file size to a point where system performance is affected, and these records should be first retried then deleted. In general, perform a download cleanup when the PUBLIC.download table reaches 80% of the expected number of rows, or if it has been necessary to make a significant number of database changes. Monitor this table using Display Database Statistics [dbstats].

If you use a large number of intelligent devices, then this table should be checked frequently. A typical time period for cleaning the download table is once per month. Download records are not automatically deleted upon successful transfer.

ACCESS CONTROL TRANSACTION ARCHIVING [accsarch]

Archiving transfers information from the system hard disk to tape, freeing up space on the hard disk for new data. Archiving should be performed regularly to ensure disk integrity. Perform an archive when the PUBLIC.archist table reaches 80% of the expected number of rows. Monitor this table using *Display Database Statistics* [dbstats]. Archiving is usually performed monthly or every two months. Note that unless necessary for reporting purposes, WSE recommends that you archive system information when your transaction volume reaches 100,000 records.

ALARM TRANSACTION CLEAN UP [alrmcln]

Each time an alarm is triggered, a record is created and stored in a separate file along with the operator's alarm servicing response. This table is then available for reporting using the alarm servicing report. Over time, the size of this table grows and takes up excessive space on the hard disk. Cleanup this table when the PUBLIC.alrmtran table reaches 80% of the expected number of rows. Monitor this table using *Display Database Statistics* [dbstats].

JOURNAL ARCHIVE [jourarch]

This function copies journal records to tape and then deletes them from the hard disk. The journal archive program archives all journal information except for the current day. Archiving is performed using the [jourarch] screen:

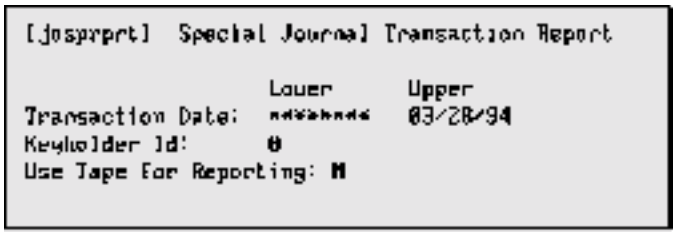
JOURNAL REPORTING [jourrprt]

This function reports all changes to the database. The report prints the column name and value for each field of each record that has been entered. With updates, the report shows the record before and after the change. Associated operator, and date and time are also reported. A sample report follows:

```
04/02/96                        De Quincy Laboratories              Page   1
12:14                           Audit Trail Report

Operator          Table              Date           Time          Operation Type
________________  _____________      ________       _____         ____________________
jon               cards              04/02/96       12:07         Add
upbzone:   -1
ppbzone:   -1
keyisalt:  NULL
priv: N
```

SPECIAL JOURNAL REPORTING [josprprt]

This function produces a formatted history report of all database changes to the keyholders and keyholder access assignment Information. Sample screens and reports follow:



KEYHOLDER LOADING [loadmenu]

This function copies keyholder IDs and names from an DOS ASCII file to a Unix then creates keyholder records. The format of records in the ASCII file must be as follows:

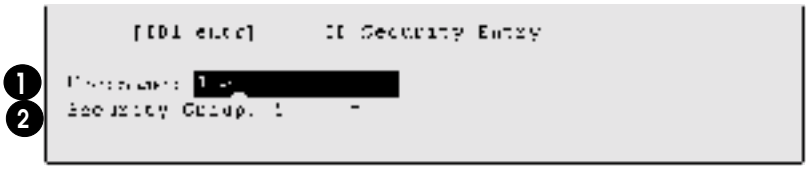
- Keyholder ID ^ALastname ^AFirstname (^A refers to a single control-A character)
- Keyholder ID 1 to 9 digits; both name fields 15 characters maximum

ID SECURITY MAINTENANCE [ID_menu]

The ID Security Maintenance function controls access to the information shared by the SE 6000 and the Polaroid ID-4000 Identification System. It also controls access to selected fields in the keyholder record. Add/update functions within the key enter and key-1 enter screen can be regulated by user ID.

ID SECURITY USER ENTRY [ID1_ entr]

ID Security Maintenance data is created via the ID Security Maintenance menu:

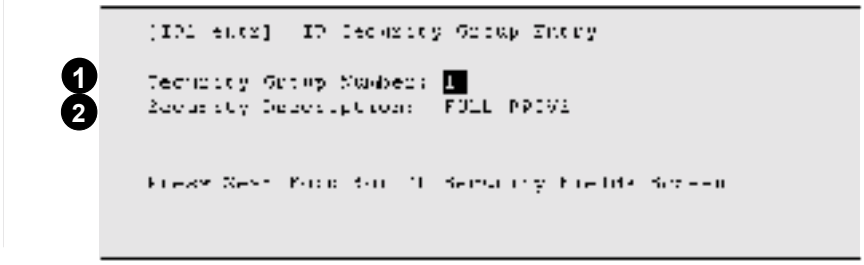


Required. Enter the user name.

Required. Enter the user's security group number. With the SE 6000, ID security groups must exist (or be created via the ZOOM function) before the system administrator can complete user entry.

ID SECURITY GROUP ENTRY [ID2_ entr]

This function is used to create ID security groups. A sample screen follows:

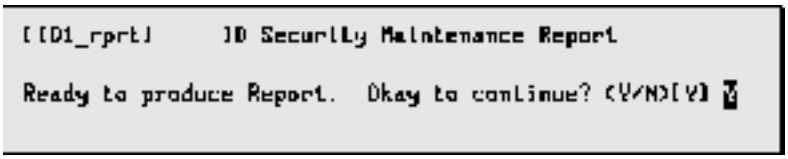


Required. Enter a unique security group number in the range 1—999.

Optional. Enter a group description (30 characters maximum).

ID SECURITY REPORT [ID1_ rprt]

This function is used to prepare a report showing all users entered into the ID security feature, along with tenant and group definition information. A sample of a partial screen and report follow:




```
06/26/96                    Campbell Engineering
07:26                       ID Security Maintenance Report          Page 1
Login Name      Tenant  Tenant Name             Group  Group Name              Add    Del
_____________   ______  ______________________  _____  ______________________  ___    ___

JERID                0  All Encompassing       1      Complete Record Access  Y      Y

                            Field                     View  Modify
                            ______________________    ____  ______

                            Keyholder ID               Y     Y
                            Tenant Number              Y     Y
                            Key Number                 Y     Y
                            Company                    Y     Y
                            Dept                       Y     Y
```

MISCELLANEOUS INFORMATION

ADJUSTABLE BAUD RATE—708P / 800 POLLERS

Multiple baud rates are supported for the diverse mix of communications equipment available for the SE 6000 system. The baud rate is set by changing the HOSTBAUD parameter in the $DATAPATH/NPOLLER.*x* file where *x* is the associated poller number. The baud rate is entered during installation or changed as needed by the system administrator; operator action is not required. The baud rate options are:

Parameter missing — HOSTBAUD defaults to 4 (9600 bps)
HOSTBAUD=4 — 9600 bps
HOSTBAUD=3 — 4800 bps
HOSTBAUD=2 — 2400 bps
HOSTBAUD=1 — 1200 bps
HOSTBAUD=0 — 300 bps

NOTE

1. The baud rate set applies to *all* devices controlled by the poller.

2. Though functional, the 300 bps baud rate (HOSTBAUD=0) is not recommended for the 800-series devices. The amount of data downloaded to intelligent ACUs significantly impacts overall system performance when inefficient communication facilities are used.

3. On 708P ACUs, the host port speed on the device is set with dipswitches. Both the device and the poller must be set for the same speed.

708P REX SHUNT TIME RESET

The normal operation of a REX switch is to shunt an associated door switch when opening the door from the nonreader controlled side, or —and in addition— to automatically unlock the door. Once the door switch is toggled, a DOOR HELD OPEN message is generated if the door is not closed within the time defined in the door switch point record.

Designed for high-traffic areas, this feature enhances the REX / Door switch functionality by providing a method to reset the door switch timer while the door is being held open. While employees continue to present valid keys and to pass through the door (causing the REX point to continually change state), the door switch timer is reset each time to the number of seconds in the door switch point record, thus preventing a DOOR HELD OPEN message from being generated. (The message *is* generated if the time between key presentation exceeds the time value in the record.)

This feature is enabled / disabled using the REXEXTEND parameter in the $DATAPATH/NPOLLER.*x* file where *x* is the associated 708P poller number. The feature is enabled / disabled during installation, or may be changed as needed by the system administrator. If changed, the poller must be halted and restarted for the parameters to take effect. The recognized REXEXTEND values are:

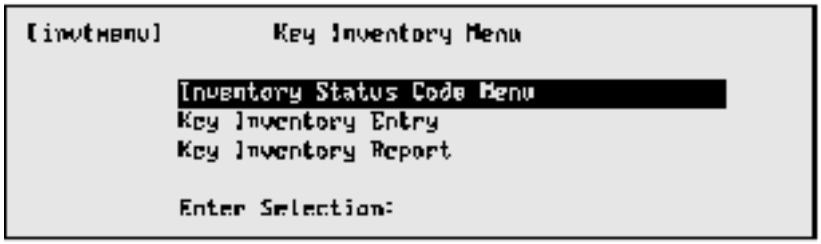
Parameter missing — REXEXTEND defaults to 0 (feature disabled)
REXEXTEND=0 — Feature disabled
REXEXTEND=1 — Feature enabled

NOTE

The enable / disable condition as set applies to *all* devices controlled by the poller.

KEY INVENTORY [invtmenu]

This feature is used to control system keys. This is an optional feature and does not effect operation. The menu screen is accessed from the main menu:



INVENTORY STATUS CODE MENU [statentr]

Key codes and descriptions are selected by the user (Code 1=*Key in use* is frequently set). Other code descriptions could be: *Key available*, *Key damaged*, *Key issued*, *Key lost*, *Key reported stolen*. In most cases, from four to ten (maximum) are set. The key codes and descriptions are entered using the key inventory status code entry screen:

KEY INVENTORY STATUS CODE REPORT [statrprt]

This report lists established key codes (for a current key status report, see *Key Inventory Report* (following subsection). A sample screen and report follow:

```
[statrprt]   Inventory Status Code Report

Ready to produce Report. OK to continue? (Y/N)(Y)
```

```
03/25/96                    Ataraxia Electronics                    Page 1
15:52                       Inventory Status Code Report

  Code    Code Description
  ____    ________________
     1    AVAILABLE
     2    ASSIGNED
     3    LOST
     4    UNUSABLE
     5    DAMAGED
     6    TERMINATED
     7    REISSUED
     8    RECOVERED
     9    PREVIOUS OWNER
    10    RESERVED
```

KEY INVENTORY ENTRY [cdinentr]

This function is used to add/change key inventory information (to delete a key record, use the system delete record feature — Esc, d, r):

```
[cdinentr]                Key Inventory Entry

Key Type : 1    Facility Code : 0034    Key # : 30463

Kyhldr ID: 7          Lastname: AUSS          Firstname: AMOV
Tenant   : 0    = BU[LD]NG ADM]N]STRAT[ON
Status   : 2    = ASS]GNED
Date     : 05/08/92
Time     : 15:16
Remarks  :
```

KEY INVENTORY REPORT [cdinrprt]

A sample screen and report follow:

```
[cdinrprt]       Key Inventory Report

                      Lower Limit   Upper Limit
    Key Number   :    3
    Keyholder ID :
    Tenant Number:


    Sort Sequence:              1) Name, Keyholder ID
                                2) Keyholder ID
```

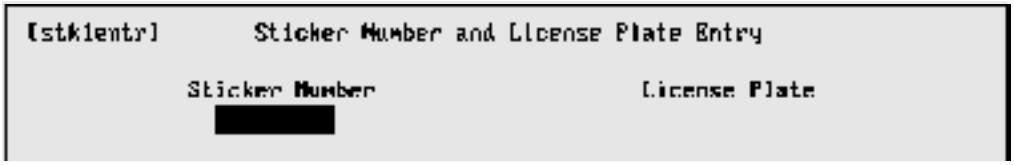
```
03/25/96                          Alpha Systems                          Page  1
15:55                             Key Inventory Report

 Keyholder   Keyholder Name          Key No   Date       Time     Status Descrip        Remarks
 _________   ____________________    ______   ________   _____    __________________    ________

     29205   THORPE JAMES            29606   06/23/96   13:15    ASSIGNED
     31408   ROSS MICHAEL            31409   06/23/96   13:22    ASSIGNED
     33244   DESJARDINS ROBERT       33249   06/23/96   13:25    ASSIGNED
     36427   JERRY TIMOTHY           36426   06/23/96   13:44    ASSIGNED
     37441   JUDD AL                 37444   06/23/96   13:51    ASSIGNED
```

PARKING STICKERS [stkrmenu]

This feature is used to control parking stickers issued to keyholders. The initial screen is accessed from the main menu:

PARKING STICKER ENTRY [stkrentr]

Enter the required information; the second parking entry screen automatically displays:



PARKING STICKER INTERACTIVE DISPLAY [stkrrprt1]

This function is used to determine keyholder location. Enter the keyholder ID; the location data displays automatically:

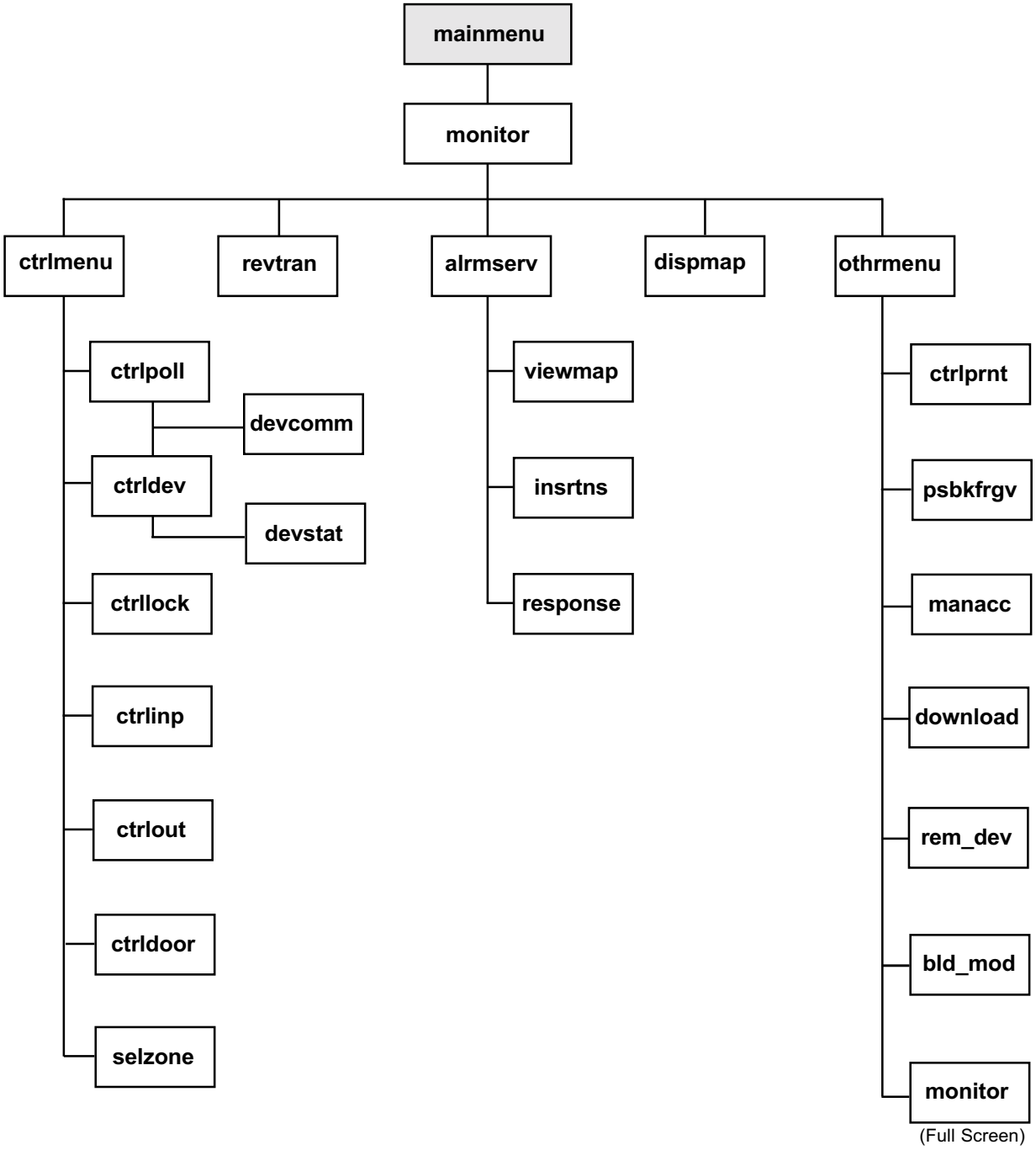
```
[stkrprt1]      Parking Sticker Interactive Display

                      Keyholder ID: 000066103

Last Name: TIM              First Name: D+NP              Visitor: N
        Company  : 3    = WESTINGHOUSE SECURITY ELEC.
        Dept     : 3    = ENGINEERING
        Location : 2    = SANTA CLARA, CA - TECHMART BLD
        Phone    : 408 727-5178
```

PARKING STICKER MASTER REPORT [stkrprt]

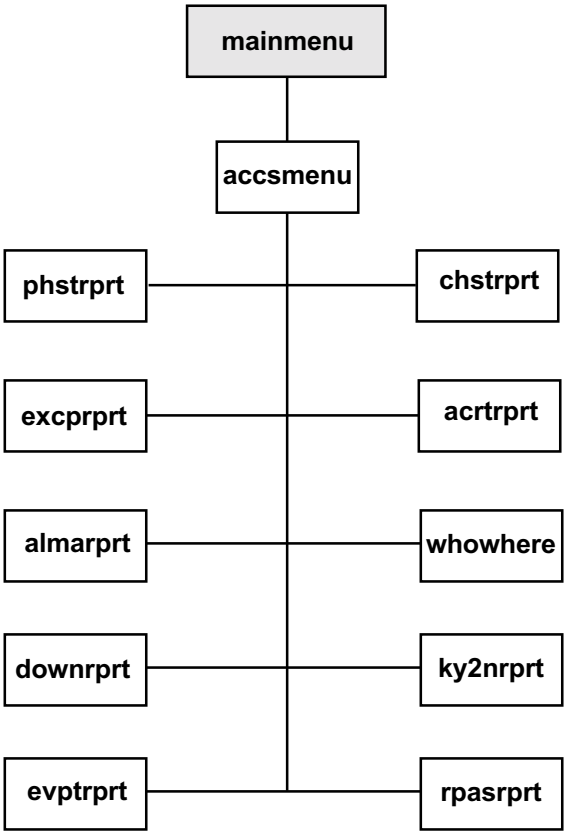
The report lists assigned parking stickers. A sample screen and report follow:

```
[stkrprt]    Parking Sticker Master Report

Sort Sequence: 2

     (1=Keyholder ID;  2=Last Name;  3=Sticker Number)
```

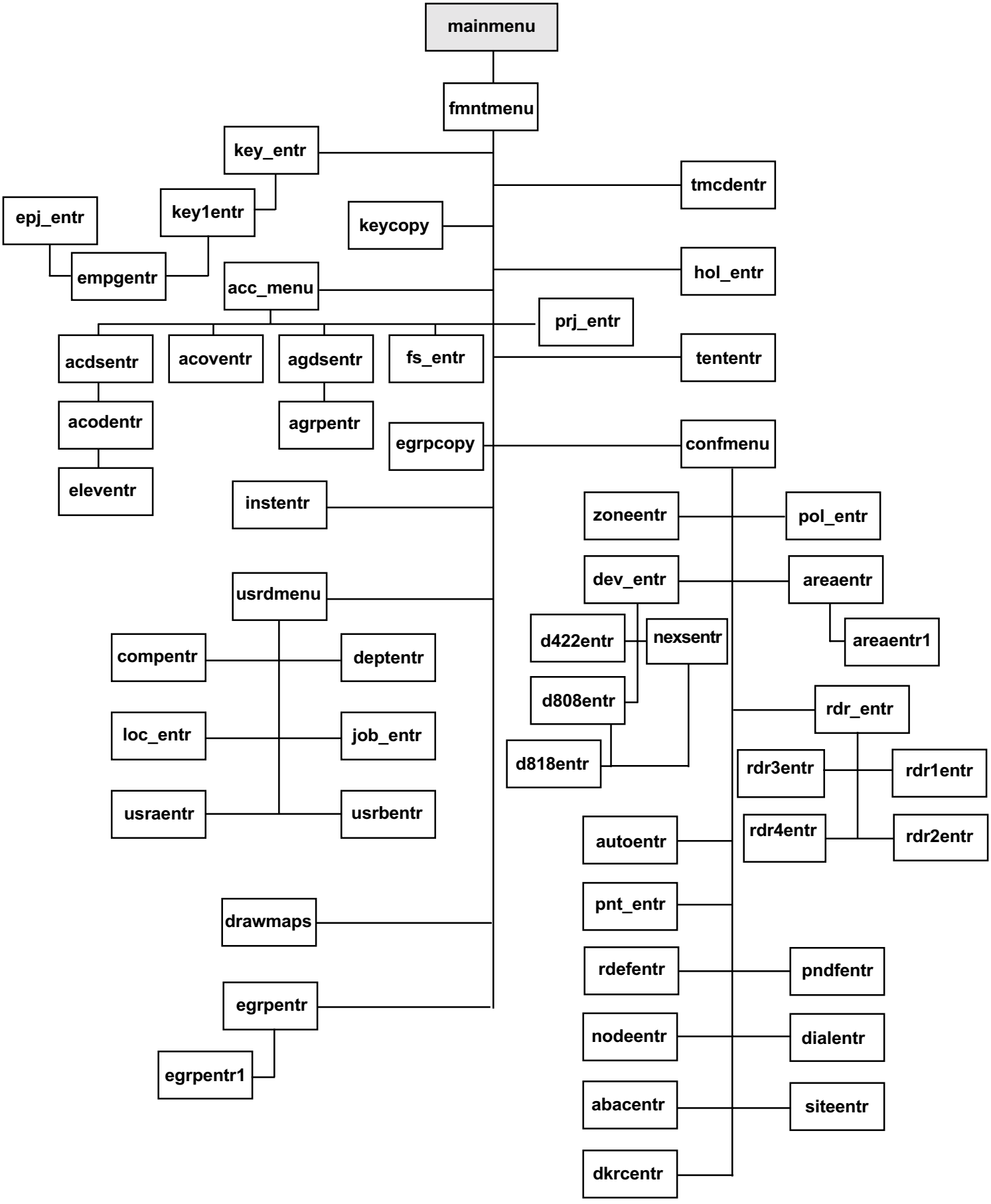
```
06/25/96                    Security Electronics              Page  1
16:00                       Parking Sticker Report

  Keyholder   Keyholder Name                          Sticker  License
  _________   ___________________________________     _______  _______

      28870   TERRY VALE                               500003  2MJK239
      28977   JESS WHITTINGTON                         500031  4B03048
      28993   CHERYL ROBERTS                           500032  4888308
      29001   PETER VAUGHAN                            500001  2PQS707
```



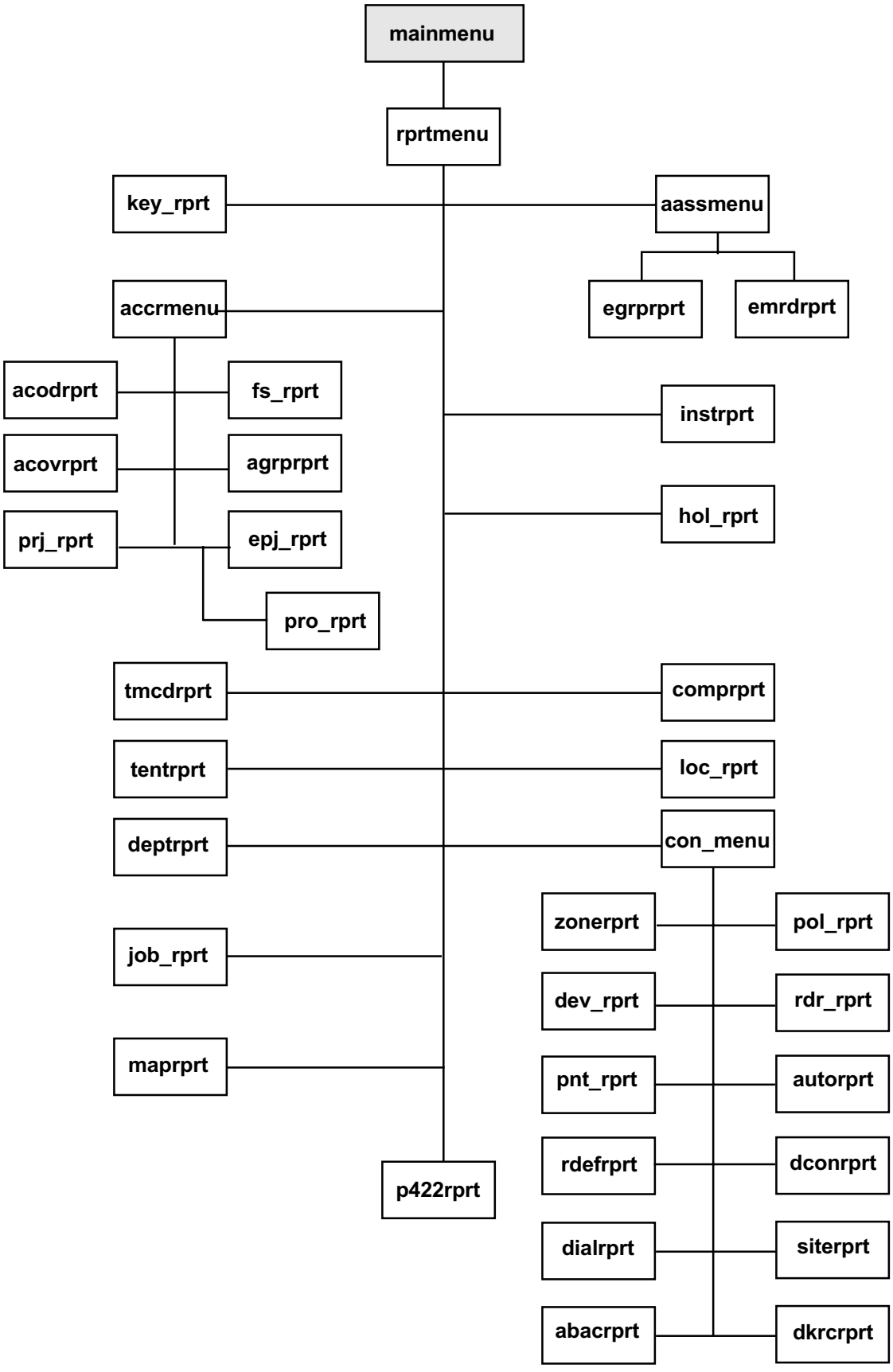
Screen Location Tree — Monitor Security Activity



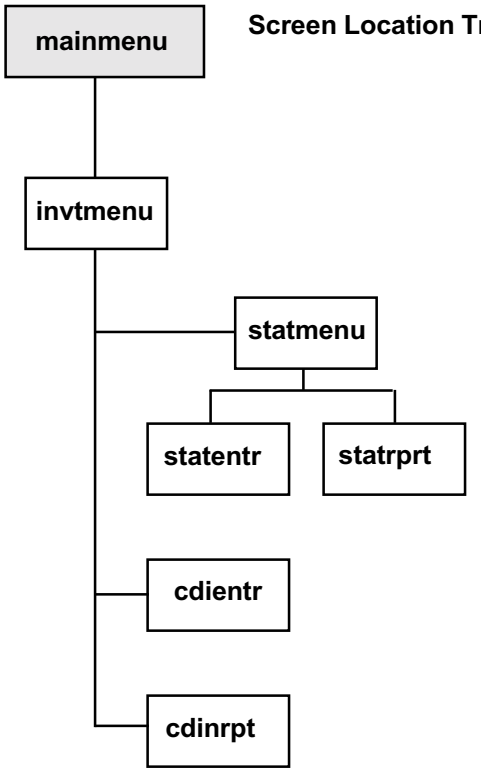
Screen Location Tree — Security Management Reports



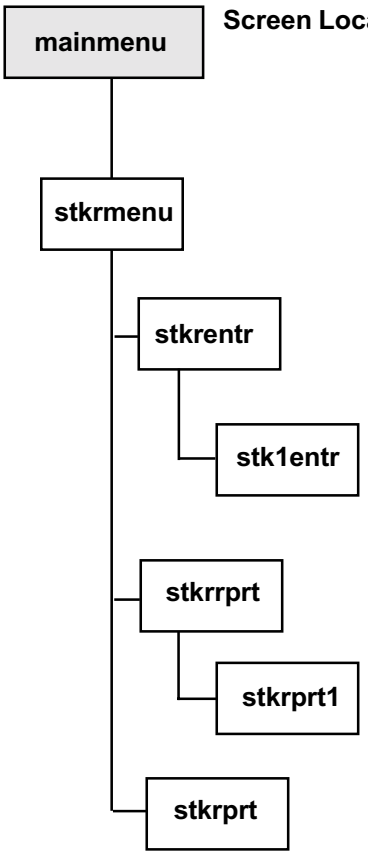
Screen Location Tree — Master File Entry



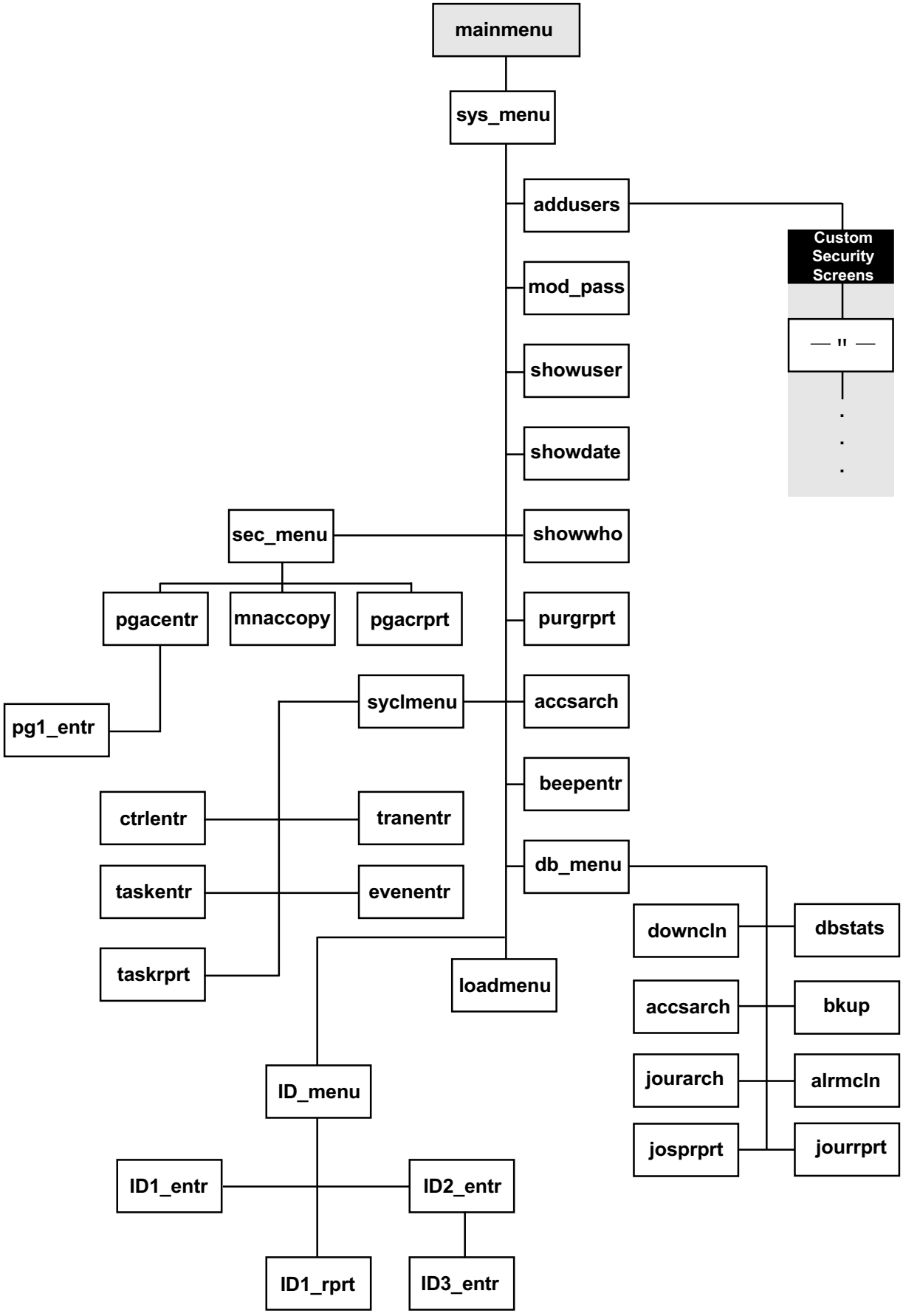
Screen Location Tree — Master File Reports



Screen Location Tree — Key Inventory



Screen Location Tree — Parking Stickers



Screen Location Tree — System Administration

MONITOR SECURITY ACTIVITY

SCREEN TITLE	FUNCTION
monitor	Watch events and activities as they occur; menu to other monitoring and control screens.
ctrlmenu	Menu to control functions. Zone selection stays in effect until this screen is exited.
ctrlpoll	Select pollers to halt or restart, and to check device communication.
devcomm	Check communication between computer and attached devices.
ctrldev	Select devices to reset / shunt / unshunt, and to check status.
devstat	Check point status for a particular device.
ctrllock	Select locks to open, lock, time open, shunt, unshunt.
ctrlinp	Select input points to shunt, unshunt.
ctrlout	Select output points to activate, deactivate, shunt, unshunt.
ctrldoor	Select door switch points to view status, shunt, unshunt.
selzone	Select zone to which the control and monitoring will be limited.
revtran	Page forwards / backwards through the last 5,000 system transactions.
alrmserv	Display currently pending alarms; provides response instructions, map.
viewmap	Display user-created map showing alarm locations.
insrtns	Display user-created list of actions to be taken when an alarm occurs at a specific point.
response	View copy of alarm instructions; enter actions taken in response to the alarm.
dispmap	Display user-created system maps showing alarms, door status, lock status, etc.
othrmenu	Menu to several system control functions.
ctrlprnt	Reset, turn on, turn off system log printers.
psbkfrgv	Restore passback status for a single keyholder, or for all keyholders in the system.
manacc	Allow entry for keyholder who does not have a key (operator and keyholder data logged).
download	Extract database information, then update memory for host and attached devices.
rem_dev	Establish connection with a remotely connected device.
bld_mod	View and control building modes for individual ACUs or all ACUs in a zone.
monitor	Provides a full-screen display (22 lines) of real-time transactions.

SECURITY MANAGEMENT REPORTS

SCREEN TITLE	FUNCTION
accsmenu	Menu to the security management reporting functions.
phstrprt	Report last twenty activities which took place at a specific point.
chstrprt	Report last twenty activities which took place for a specific keyholder.
excprprt	Report transactions currently stored on the hard disk.
acrtrprt	Report transactions currently stored on tape.
almarprt	Report of operator responses to alarms.
whowhere	Report number of keyholders in each passback level.
downrprt	Report database changes. Serves also as an audit trail of operator activity.
k2nrprt	Report last zone entered (summary or detail). Uses keyholder history as source.
evptrprt	Report system events — totals for each event within a selected date range.
rpasrprt	Report real-time zone passback activity showing how many and / or who is currently in which zone. Uses shared memory data as source.

MASTER FILE ENTRY

SCREEN TITLE	FUNCTION
key_entr	Enter primary keyholder information: keyholder ID, key number, name, tenant, etc.
key1entr	Enter keyholder personal information: address, phone, title, floor, remarks, etc.
empgentr	Assign access privileges to a keyholder.
epj_entr	Assign projects to a keyholder.

key_copy	Create new keyholder record by copying from an existing keyholder record.
egrpentr	Select a keyholder for access privilege assignment. Can also be reached from key1entr.
egrpentr1	Assign access privileges to a keyholder.
egrpcopy	Copy one keyholder's information to another keyholder.
acc_menu	Menu to reach the access definition functions.
acdsentr	Enter / modify access code information.
acodentr	Add key readers to an access code.
eleventr	Enter elevator output contact information for a specific reader in a specific access code.
acoventr	Temporarily override keyholder or keyholder group access.
agdsentr	Enter / modify access groups.
agrpentr	Add access codes to an access group.
fs_entr	Enter / modify fail-soft access capabilities for a 708P.
prj_entr	Define projects, start / stop dates and times.
tmcdentr	Enter / modify time code information.
hol_entr	Enter / modify holiday information.
tententr	Enter / modify tenant information.
instentr	Enter / modify alarm point information
confmenu	Menu to the system configuration functions.
zoneentr	Enter / modify zone information.
areaentr	Enter / modify areas.
areaentr1	Enter / modify zones in areas.
pol_entr	Enter / modify poller information.
dev_entr	Enter / modify device information .
nexsentr	Enter / modify information specific to NexSentry.
d808entr	Enter / modify information specific to 808S.
d818entr	Enter / modify information specific to 818x.
d422entr	Enter / modify information specific to SE 422.
rdr_entr	Enter / modify reader / key pad information.
rdr1entr	Enter / modify reader information specific to 808S.
rdr2entr	Enter / modify reader information specific to SE 422.
rdr3entr	Enter / modify reader information specific to 818x.
rdr4entr	Enter / modify reader information specific to NexSentry.
pnt_entr	Enter / modify point information.
autoentr	Enter auto-activation / auto-opening times for points / readers.
rdefentr	Define 808S action reports.
pndfentr	Define default number of digits and seed the PIN (SE 422).
nodeentr	Enter / modify sub-device information for SE 422.
dialentr	Enter / modify remotely connected device information.
siteentr	Define site configuration for SE 422.
abacentr	Define ABA (magnetic stripe card) configuration.
dkrcentr	Define digital key reader configuration.
usrdmenu	Menu to the user-defined field entry screens.
compentr	Enter / modify user-defined field A (appears on key_entr).
deptentr	Enter / modify user-defined field B (appears on key_entr).
loc_entr	Enter / modify user-defined field C (appears on key_entr).
job_entr	Enter / modify user-defined field D (appears on key_entr).
usraentr	Enter / modify user-defined field E (appears on key_entr).
usrbentr	Enter / modify user-defined field F (appears on key_entr).
drawmaps	Create real-time control maps / alarm location maps.

MASTER FILE REPORTS

SCREEN TITLE	FUNCTION
rprtmenu	Menu to database reporting functions.
key_rprt	Report keyholder information.
aassmenu	Menu to the access assignment reporting functions.
egrprprt	Report access codes / access groups assigned to keyholders.
emrdrprt	Report specific readers assigned to keyholders.
accrmenu	Menu to the access definition reporting functions.
acodrprt	Report readers and time codes for the access codes.
agrprprt	Report access assignments for access groups.
acovrprt	Report access override data.
fs_rprt	Report fail-soft access privileges for 708P.
prj_rprt	Report all projects.
epj_rprt	Report all keyholders assigned to projects.
pro_rprt	Report all projects / readers included in individual projects.
tmcdrprt	Report all time codes.
hol_rprt	Report all defined holidays.
tentrprt	Report all defined tenants.
comprprt	Report all user-defined field A information.
deptrprt	Report all user-defined field B information.
loc_rprt	Report all user-defined field C information.
job_rprt	Report all user-defined field D information.
instrprt	Report all alarm instructions.
map_rprt	Report all map names for specific point IDs.
con_menu	Menu to the system configuration reporting functions.
zonerprt	Report all defined zones.
pol_rprt	Report all defined pollers.
dev_rprt	Report all defined device information.
rdr_rprt	Report all defined readers.
pnt_rprt	Report all point information
autorprt	Report all point / reader auto-activate / auto-open information
rdefrprt	Report all defined 808S action report information.
dconrprt	Report all remotely connected devices.
dialrprt	Report all remote site information.
siterprt	Report all defined ABA sites
abacrprt	Report all defined ABA configurations.
dkrcrprt	Report all digital key reader information.
p422rprt	Report all keyholders for SE 422 (detailed or summary).

KEY INVENTORY

SCREEN TITLE	FUNCTION
invtmenu	Menu to key Inventory functions.
statmenu	Menu to the status definition functions.
statentr	Enter key inventory status codes.
statrprt	Report all inventory status codes.
cdinentr	Enter key data.
cdinrprt	Report inventory information for all keys.

PARKING STICKERS

SCREEN TITLE	FUNCTION
stkrmenu	Menu to parking sticker and license plate management functions.
stkrentr	Select keyholder for parking sticker and / or license plate information entry.
stk1entr	Enter parking sticker or license plate information for keyholder.
stkrrprt	Locate keyholder by license plate or parking sticker.
stkrrprt1	Display keyholder location information by license plate or parking sticker number.
stkrprt	Report all parking sticker / license plate information.

SYSTEM ADMINISTRATION

SCREEN TITLE	FUNCTION
sys_menu	Menu to the system administration functions.
addusers	Add operator to system.
mod_pass	Change operator passwords.
sec_menu	Menu to the security level definition functions.
pgacentr	Create / modify security levels.
pg1_entr	Add / modify screen information for a particular security level.
mnacopy	Create new security level by copying existing security level then modifying.
pgacrprt	Report all defined security levels.
showuser	Display all system operators.
showdate	Display current system date and time.
showwho	Display operators currently using the system.
purgrprt	Cancel submitted reports.
beepentr	Define terminals for alarm response (beep) regardless of system area where operating.
syclmenu	Menu to system configuration functions
ctrlentr	Change report titles / user-defined fields. Define terminal for automatic alarm response.
evenentr	Enter / modify event information.
taskentr	Enter / modify task information.
taskrprt	Report all tasks / events.
tranentr	Enter / modify transaction information (controls data display and storage).
dbmenu	Menu to the database administration functions.
dbstats	Display size of database tables (determines if archiving is required).
bkup	Backup database to tape.
downcln	Remove unwanted records from the download file.
accsarch	Transfer records from disk to tape to free up disk space.
alrmcln	Remove operator responses to alarms from disk to free up disk space.
jourarch	Copy journal records to tape and remove from disk.
jourrprt	Report history of all database changes.
josrprt	Report history of all changes to keyholder and keyholder access assignment information.
loadmenu	Load keyholder information from ASCII files.
ID_menu	ID security maintenance menu for WSE ID-4000 interface option.
ID1_entr	Enter users, passwords, and privileges for WSE ID-4000 operators.
ID2_entr	Define security groups for WSE ID-4000 operators.
ID3_entr	Define specific operator privileges for a security group.

#	Message	Explanation
0	**Negative Acknowledge**	708P unable to understand message from host.
1	**Access Granted**	Card or keypad entry granted access by ACU or host.
2	**Key Trace**	Card flagged as TRACE has been read.
3	**Point Trace**	A card has been read by a sensor flagged as TRACE.
4	**Invalid Time**	Access denied — card not valid at that time.
5	**Invalid Day**	Access denied — card not valid that day.
6	**Invalid Reader**	Access denied — card not valid at that sensor.
7	**Key Not Active Yet**	Access denied — card presented prior to issue date.
8	**Key Terminated**	Access denied — card presented after return date.
9	**Point Disabled**	Access denied — sensor disabled.
10	**Point Not On File**	Sensor or point not defined in the host computer.
11	**Key Not On File**	Access denied — key not in ACU or host memory.
12	**Invalid Facility Code**	Access denied — wrong facility code (1030/1040 keys only).
13	**Manual Unlock**	Reader / door manually unlocked.
14	**Manual Lock**	Reader / door manually locked.
15	**Auto Unlock**	Reader / door auto-unlocked by host or ACU.
16	**Auto Lock**	Reader / door auto-locked by host or ACU.
17	**Door Forced Open**	Door with status switch opened without card or REX.
18	**Door Held Open**	Door with status switch remains open beyond set time.
19	**Door Closed (Forced)**	Forced door has now been closed.
20	**Door Closed (Held)**	Door held open too long has now been closed.
21	**Access Requested**	Valid key presented; host waiting for corresponding keypad entry
22	**Poller Died**	Software poller has failed.
23	**Poller Can't Open Port**	Hardware poller has failed (poller device open error).
24	**Poller Started**	Poller started.
25	**Poller Stopped**	Poller stopped.
26	**Host Comm. Started**	Communication initiated between host and LC / RLC.
27	**Host Comm. Stopped**	Communication ended between host and LC / RLC.
28	**Printer Off**	Log printer switched off.

#	Message	Explanation
29	**Printer On**	Log printer switched on.
30	**Device Reset**	708P / 8xx-series powered up / re-initialized.
31	**Return From Failsoft**	708P communication restored — no longer in failsoft mode.
32	**Power Failed**	708P / 8xx-series with 3708 UPS has lost AC power.
33	**Power Restored**	708P / 8xx-series with 3708 UPS has regained AC power.
34	**Tamper Active**	708P / 8xx-series tamper input active.
35	**Tamper Clear**	708P / 8xx-series active tamper input now cleared.
36	**COAX Failure**	Coax cable from ACU to reader shorted.
37	**COAX OK**	Coax cable from ACU to reader repaired.
38	**Sensor Failure**	ACU has lost communication with reader (open coax).
39	**Sensor OK**	Previously failed reader (or open coax) repaired.
40	**Printer Error**	Log printer is not functioning properly.
41	**Poller Params Reloaded**	Host has initialized a poller.
42	**Still Held Open**	DOOR HELD OPEN — Second alert message.
43	**Input Point Active**	A GENERAL input has been activated.
44	**Input Point Normal**	Previously activated GENERAL input point has been cleared.
45	**Timeout Device**	Response from polled ACU by host not received within allotted time (usually 2 seconds).
46	**Unable to Lock Door**	Host unable to implement automatic or manual command to lock a door (error on lock).
47	**Unable to Unlock Door**	Host unable to implement automatic or manual command to unlock a door (error on unlock).
48	**Unable to Clear Output**	Host unable to restore output contact to normal (error on output clear).
49	**Unable to Act. Output**	Host unable to restore output contact to active (error on output clear).
50	**Not Used**	Reserved for future applications.
51	**Not Used**	Reserved for future applications.
52	**Manual Unlock Timed**	Timed unlock command entered.
53	**Manual Access Granted**	Manual access command issued.

#	Message	Explanation
54	**Device Online**	ACU communicating with host.
55	**Request Manual Access**	Manual access command entered.
56	(Building Closed Trace)	Obsolete message
58	**Repack OK**	Host has loaded new database information.
59	**Error Setting Bldg. Mode**	Building mode command unsuccessful.
60	**Key Activated**	Key presented to activate reader — activate card enabled.
61	**Key Deactivated**	Key presented to deactivate reader — deactivate card enabled.
62	**Key Not Active**	Access denied — key applies to activate reader.
63	**New Day**	Host rebooted or clock has crossed 00:00.
64	**Remote Trans Received**	Dial-up device transmission received by host.
65	**Host Dial OK**	Host has called a dial-up device.
66	**Error Dialing Remote**	Download errors to remote dial-up device encountered.
67	**Output Activated**	Output contact manually or automatically activated.
68	**Output Deactivated**	Output contact manually or automatically deactivated.
69	**Invalid PIN Entered**	PIN entered incorrect.
70	**Redundancy On**	Not used at this time.
71	**Redundancy Off**	Not used at this time.
72	**Host Poller Down**	Not used at this time.
73	**Acknowledge DB Xfer**	Data successfully downloaded to target device.
74	**Failed DB Xfer**	Data download attempt to target device failed.
75	**No Key Set for PIN**	PIN entered without valid key presentation.
76	**Keyholder Duress**	PIN entered in reverse sequence indicating a duress situation. If valid, access is granted.
77	**Controller Comm Error**	Host to local controller communication failed.
78	**RDI Dialed In**	RDI unit has dialed host and is logged in.
79	**Lot Full**	Optional parking function.
80	**Max Tenant In Lot**	Optional parking function.
81	**Alarm Resolved**	Alarm event resolved.
82	**Enter Attended Mode**	Optional parking function.

#	Message	Explanation
83	**Enter Unattended Mode**	Optional parking function.
84	**Batch Request Received**	Not used at this time.
85	**Remote Comm Ended**	Not used at this time.
86	**Global Silence Request**	Silence global beeping command issued.
89	**Ticket Serviced**	Parking application has completed ticket update/storage activities.
90	**Chksum Err In Sys DB**	Difference exists between host and ACU system data.
91	**Chksum Err In Key DB**	Difference exists between host and ACU key data.
92	**Alarm Active**	Alarm input active.
93	**Alarm Clear**	Previously active alarm input cleared.
94	**Shunt Point**	Device / point shunt command issued.
95	**Unshunt Point**	Device / point unshunt command issued.
96	**Not Used**	Reserved for future applications.
97	**Parameter Load Error**	Host poller initialization failed.
98	**Tran File Almost Full**	Archive history file approaching capacity. Archive immediately.
99	**Database Error**	Data to database failed. There may be many possible causes.
100	**Passback Violation**	Access denied — passback status.
103	**Building Open**	808-series — ACU in open mode.
104	**Building Open Limited**	808-series — ACU in limited mode.
105	**Building Closed**	808-series — ACU in closed mode.
106	**Tamper Report Shunted**	8xx-series ACUs — device tamper report is shunted.
107	**Tamper Report Unshunt**	8xx-series ACUs — device tamper report is unshunted.
108	**Request To Exit**	REX contact activated during valid REX time.
109	**REX Denied**	REX contact activated during invalid REX time.
110	**MSM Fail**	MSM failed.
111	**MSM Okay**	Previously failed MSM repaired.
112	**Door Report Shunted**	Door forced report shunted.
113	**Door Report Unshunted**	Door forced report unshunted.
114	**Power Report Shunted**	Device power fail report shunted.

#	Message	Explanation
115	**Power Report Unshunted**	Device power fail report unshunted.
116	**COAX Report Shunted**	Reader coax fail report shunted.
117	**COAX Report Unshunted**	Reader coax fail report unshunted.
118	**Sensor Report Shunted**	Sensor / reader fail report shunted.
119	**Sensor Report Unshunted**	Sensor / reader fail report unshunted.
120	**MSM Report Shunted**	8xx-series ACU MSM fail report shunted.
121	**MSM Report Unshunted**	8xx-series ACU MSM fail report unshunted.
122	**Power Report Shunted**	8xx-series ACU MSM power fail report shunted.
123	**Power Report Unshunted**	8xx-series ACU MSM power fail report unshunted.
124	**Bldg Opened**	8xx-series ACU MSM power fail report shunted.
125	**Bldg Opened Limited**	8xx-series ACU placed in limited mode.
126	**Bldg Closed**	8xx-series ACU placed in closed mode.
127	**Bldg Should be Closed**	8xx-series ACU in time period where it should be closed.
128	**Can't Close Bldg (Key)**	8xx-series ACU cannot be placed in closed mode because proper key not presented.
129	**Can't Close Bldg - User**	8xx-series ACU cannot be placed in closed mode because of user actions.
130	**Terminal Buffer Full**	8xx-series host port log buffer at capacity.
131	**Device Cannot Connect**	8xx-series ACU unable to communicate with host / dial-up interface.
132	**Alarm Silenced**	8xx-series ACU silenced by a user connected through the ACU terminal port.
133	**Forgive Passback**	Passback status on card / card group set to unknown.
134	**Invalid T & A Request**	No longer used.
135	**Time & Attendance Clock**	Key presented at a valid time and attendance reader.
136	**Meal Counter - Excp.**	Keyholder over meal limit.
137	**Meal Counter - Valid**	Key presented at valid meal counter reader.
138 *and* **139**		Reserved for future applications.
140	**User Logged Into Term**	User logged on to 8xx-series ACU via the terminal port.
141	**User Logged Off Term**	User logged off an 8xx-series ACU via the terminal port.

#	Message	Explanation
142	**Host Dial Start**	Remote device dialing host.
143	**Carrier Off**	SE 422—Incoming phone line or host port has lost DTR.
144	**Carrier On**	SE 422 — Incoming phone line or host port DTR high.
145	**Logs Purged**	SE 422 — Log buffer purged.
146	**Threshold Met**	SE 422 — Logs have met user-defined threshold.
147	**Deferred Key**	Key referred to host for access decisions.
148	**Auto Forgive**	Automatic forgive passback issued.
149	**Zone Count Reset**	Count for a particular zone or all zones reset.
150	**Req. Passback Forgive**	Forgive passback command issued.
151	**Timer Started**	Not used at this time.
152	**Timer Cancelled**	Not used at this time.
153	**Timer Expired**	Not used at this time.
154	**Request Reset Device**	Operator initiated device reset from devices menu.
155	**Request Reset Keys**	Operator initiated key reset from devices menu.
156	**Reset Device Okay**	Affirmative response following device reset command.
157	**Reset Key Okay**	Key information successfully reset in 8xx-series ACU.
158	**Error on Device Reset**	Unable reset memory / system data for 8xx-series ACU.
159	**Error on Key Reset**	Unable reset key data for 8xx-series ACU.
160	**Open Cash Drawer**	Parking attendant cash drawer opened improperly.
161	**Invalid Card Type**	Wrong type magnetic stripe card presented.
162	**Line Cut**	SE 422 input line cut.
163	**Line Short**	SE 422 input line shorted.
164 *through* 169		Reserved for future applications.
170	**Over Device Limit**	System configuration has exceeded specified limits.
171	**Invalid Site Code**	Site code not on file or invalid.
172	**ABA Card Expired**	ABA card presented has expired.
173	**ABA Card Data 1**	Five 40-character lines (maximum) encoded on ABA cards.
174	**ABA Card Data 2**	•
175	**ABA Card Data 3**	•
176	**ABA Card Data 4**	•
177	**ABA Card Data 5**	•

#	Message	Explanation
178	**VIP Failure**	VIP keypad not responding.
179	**VIP Okay**	VIP keypad returned from failed status.
180	**VIP Tamper Fail**	VIP tamper fail reported.
181	**VIP Tamper Okay**	VIP tamper switch OK.
182	**VIP Shunted**	VIP shunted.
183	**VIP Unshunted**	VIP unshunted.
184	**VIP Tamper Shunted**	VIP tamper switch shunted.
185	**VIP Tamper Unshunted**	VIP tamper switch unshunted.
200	**Radionics Unit Test**	For Radionics systems (for future use).
201	**General Trouble**	"
202	**Zone Trouble**	"
203	**Line Card Trouble**	"
204	**General Restoral Report**	"
205	**Zone Restoral**	"
206	**Line Card Restored**	"
207	**General Opening Report**	"
208	**Zone Opening Report**	"
209	**General Closing Report**	"
210	**Zone Closed**	"
211	**General Cancel Report**	"
212	**Zone Cancel Report**	"
213	**Radionics Unit Power Fail**	"
214	**Radionics Unit Restore**	"
215	**Listen-In Report**	"
216	**Listen Done**	"
217	**Communicator Power Fail**	"
218	**Was Forced Armed**	"
219	**Status Report**	"
220	**Busy Seconds**	"
221	**Error**	"
222	**Power Up Message**	"
223	**Radionics Alarm**	"
230	**Project Activated**	Project activated.
231	**Project Deactivated**	Active project deactivated.
232	**Project Normalized**	Project normalized.
233	**Invalid Project**	Access denied to a project-controlled door (no access privileges).
240	**Alarm Not Acknowledged**	No alarm response within time specified in transaction description record.
241	**Alarm Acknowledged**	Alarm acknowledged.

#	Message	Explanation
242	**Disk Almost Full**	Disk space at value of DISKWARN parameter (usually 90% full).
250	**Over Max Key Limit**	Attempt made to download more keys than the device will hold.
300	**RDI Full**	RDI transaction buffer full.
301	**RDI Too Hot**	RDI upper temperature limit exceeded.
302	**RDI Too Cold**	RDI lower temperature limit exceeded.
303	**RDI Timeout Problem**	RDI unable to communicate with 808S.
304	**RDI Hardware Problem**	RDI has detected an error with its operating hardware.
305	**RDI Modem Problem**	RDI has detected a modem error.
306	**RDI Alarm Table Error**	RDI alarm table full or unusable.
307	**RDI Comm Error**	RDI unable to dial out.
308	**RDI Host Comm Error**	RDI unable to receive.
309	**RDI Can't Close 808 DB**	RDI unable to complete data transfer to 808S; device left in incomplete state.
500	**Debug 0 Transaction**	WSE development use only.
501	**Debug 1 Transaction**	•
502	**Debug 2 Transaction**	•
503	**Debug 3 Transaction**	•
504	**Debug 4 Transaction**	•
505	**Debug 5 Transaction**	•

Message	#
ABA Card Data 1	173
ABA Card Data 2	174
ABA Card Data 3	175
ABA Card Data 4	176
ABA Card Data 5	177
ABA Card Expired	172
Access Granted	1
Access Requested	21
Acknowledge DB Xfer	73
Alarm Acknowledged	241
Alarm Active	92
Alarm Clear	93
Alarm Not Acknowledged	240
Alarm Resolved	81
Alarm Silenced	132
Auto Forgive	148
Auto Lock	16
Auto Unlock	15
Batch Request Received	84
Below Lot Limit	88
Below Tenant Limit	87
Bldg Closed	126
Bldg Opened	124
Bldg Opened Limited	125
Bldg Should be Closed	127
Building Closed	105
Building Open	103
Building Open Limited	104
Busy Seconds	220
Can't Close Bldg (Key)	128
Can't Close Bldg - User	129
Carrier Off	143
Carrier On	144
Chksum Err In Key DB	91
Chksum Err In Sys DB	90
COAX Failure	36
COAX OK	37
COAX Report Shunted	116
COAX Report Unshunted	117
Communicator Power Fail	217
Database Error	99
Debug 0 Transaction	500
Debug 1 Transaction	501
Debug 2 Transaction	502
Debug 3 Transaction	503
Debug 4 Transaction	504
Debug 5 Transaction	505
Deferred Key	147
Device Cannot Connect	131
Device Online	54
Device Reset	30
Disk Almost Full	242
Door Closed (Forced)	19
Door Closed (Held)	20
Door Forced Open	17
Door Held Open	18

Message	#
Door Report Shunted	112
Door Report Unshunted	113
Enter Attended Mode	82
Enter Unattended Mode	83
Error	221
Error Dialing Remote	66
Error on Device Reset	158
Error on Key Reset	159
Error Setting Bldg. Mode	59
Failed DB Xfer	74
Forgive Passback	133
General Cancel Report	211
General Closing Report	209
General Opening Report	207
General Restoral Report	204
General Trouble	201
Global Silence Request	86
Host Comm. Started	26
Host Comm. Stopped	27
Host Dial OK	65
Host Dial Start	142
Host Poller Down	72
Input Point Active	43
Input Point Normal	44
Invalid Card Type	161
Invalid Day	.5
Invalid Facility Code	12
Invalid PIN Entered	69
Invalid Project	233
Invalid Reader	6
Invalid Site Code	171
Invalid T & A Request	134
Invalid Time	4
Key Activated	60
Key Deactivated	61
Key Not Active	62
Key Not Active Yet	7
Key Not On File	11
Key Terminated	8
Key Trace	2
Keyholder Duress	76
Line Card Restored	206
Line Card Trouble	203
Line Cut	162
Line Short	163
Listen Done	216
Listen-In Report	215
Logs Purged	145
Lot Full	79
Manual Access Granted	53
Manual Unlock	13
Manual Unlock Timed	52

Message	#
Max Tenant In Lot	80
Meal Counter - Excp.	136
Meal Counter - Valid	137
MSM Fail	110
MSM Okay	111
MSM Report Shunted	120
MSM Report Unshunted	121
Negative Acknowledge	0
New Day	63
No Key Set for PIN	75
Not Used	50
Not Used	51
Not Used	96
Open Cash Drawer	160
Output Activated	67
Output Deactivated	68
Over Device Limit	170
Over Max Key Limit	250
Parameter Load Error	97
Passback Violation	100
Point Disabled	9
Point Not On File	10
Point Trace	3
Poller Can't Open Port	23
Poller Died	22
Poller Params Reloaded	41
Poller Started	24
Poller Stopped	25
Power Failed	32
Power Report Shunted	114
Power Report Shunted	122
Power Report Unshunted	115
Power Report Unshunted	123
Power Restored	33
Power Up Message	222
Printer Error	40
Printer Off	28
Printer On	29
Project Activated	230
Project Deactivated	231
Project Normalized	232
Radionics Unit Power Fail	213
Radionics Unit Restore	214
Radionics Unit Test	200
RDI Alarm Table Error	306
RDI Can't Close 808 DB	309
RDI Comm Error	307
RDI Dialed In	78
RDI Hardware Problem	304
RDI Host Comm Error	308
RDI Is Full	300
RDI Is Too Cold	302
RDI Is Too Hot	301
RDI Modem Problem	305
RDI Timeout Problem	303
Redundancy Off	71
Redundancy On	70

Message	#
Remote Comm Ended	85
Remote Trans Received	64
Repack OK	58
Req. Passback Forgive	150
Request Manual Access	55
Request Reset Device	154
Request Reset Keys	155
Request To Exit	108
Reset Device Okay	156
Reset Key Okay	157
Return From Failsoft	31
REX Denied	109
Sensor Failure	38
Sensor OK	39
Sensor Report Shunted	118
Sensor Report Unshunted	119
Shunt Point	94
Status Report	219
Still Held Open	42
Tamper Active	34
Tamper Clear	35
Tamper Report Shunted	106
Tamper Report Unshunt	107
Terminal Buffer Full	130
Threshold Met	146
Ticket Serviced	89
Time & Attendance Clock	135
Timeout Device	45
Timer Cancelled	152
Timer Expired	153
Timer Started	151
Tran File Almost Full	98
Unable to Act. Output	49
Unable to Clear Output	48
Unable to Lock Door	46
Unable to Unlock Door	47
Unshunt Point	95
User Logged Into Term	140
User Logged Off Term	141
VIP Failure	178
VIP Okay	179
VIP Shunted	182
VIP Tamper Fail	180
VIP Tamper Okay	181
VIP Tamper Shunted	184
VIP Tamper Unshunted	185
VIP Unshunted	183
Was Forced Armed	218
Zone Cancel Report	212
Zone Closed	210
Zone Count Reset	149
Zone Opening Report	208
Zone Restoral	205
Zone Trouble	202

Level 1 = COMPLETE SYSTEM ACCESS

ID1_entr	ID Security User Entry	Y	Y	Y
ID1_rprt	ID Security Report	N	N	N
ID2_entr	ID Security Group Entry	Y	Y	Y
ID_menu	ID Security Report	N	N	N
aassmenu	Access Assignments	N	N	N
abacentr	ABA Configuration Entry	Y	Y	Y
abacrprt	ABA Configuration	N	N	N
acc_menu	Access Definition	N	N	N
accrmenu	Access Definition	N	N	N
accsarch	Access Ctrl Trans Arch	N	N	N
accsmenu	Security Management Rpts	N	N	N
acdsentr	Access Code Entry	Y	Y	Y
acodrprt	Access Code Master Rpt	N	N	N
acoventr	Access Override Entry	Y	Y	Y
acovrprt	Access Override Report	N	N	N
acrtrprt	Access Control Archive	N	N	N
addusers	Addusers	N	N	N
agdsentr	Access Group Entry	Y	Y	Y
agrprprt	Access Group Master Rpt	N	N	N
almarprt	Alarm Servicing	N	N	N
alotentr	Tenant Allotment	Y	Y	Y
alrmcln	Alarm Trans Clean Up	N	N	N
areaentr	Areas	Y	Y	Y
autoentr	Auto Opens / Activates	Y	Y	Y
autorprt	Auto Opens / Activates	N	N	N
badgarch	Badge Archiving	N	N	N
badgentr	Badge Entry	Y	Y	Y
badgrprt	Print Badges	N	N	N
badtrprt	Offline Badge Reporting	N	N	N
bdg1rprt	Badge Report	N	N	N
beepentr	Enable Global Beeping	Y	Y	Y
bkup	Perform Backup	N	N	N
calliq	AccellIq (Custom Reports)	N	N	N
casmrprt	Cash Summary	N	N	N
cdinentr	Key Inventory Entry	Y	Y	Y
cdinrprt	Key Inventory Report	N	N	N
chstrprt	Keyholder History Report	N	N	N
compentr	Company	Y	Y	Y
comprprt	Company	N	N	N
con_menu	Device Configuration Rpts	N	N	N
confmenu	Hardware Configuration	N	N	N
ctrlentr	Control File Maintenance	Y	Y	Y
db_menu	Database Maintenance	N	N	N
dbstats	Display Data Base Stats	N	N	N
dconrprt	808 Device Configuration	N	N	N
deptentr	Dept	Y	Y	Y
deptrprt	Dept	N	N	N
dev_entr	Devices	Y	Y	Y
dev_rprt	Devices	N	N	N
dialentr	Dialer Entry	Y	Y	Y
dialrprt	Dialers	N	N	N
dkrcentr	DKR Configuration Entry	Y	Y	Y
dkrcrprt	DKR Configuration	N	N	N
downcln	Download Clean Up & Retry	N	N	N
downrprt	Download Status	N	N	N
drawmaps	Maps	N	N	N
egrpcopy	Copy Keyholder Access	N	N	N
egrpentr	Access Assignment	Y	Y	Y
egrprprt	Keyholder Access Assign	N	N	N
emp_dnld	Keyholder Transfer	N	N	N
emrdrprt	Reader Access Assignment	N	N	N
epj_rprt	Employee Project Report	N	N	N
evenentr	Events	Y	Y	Y
evptrprt	Event / Point Report	N	N	N
excprprt	Selective Transaction	N	N	N
exit	Exit SE / SMS Application	N	N	N
fmntmenu	Master File Entry	N	N	N
fs_entr	Fail Soft Entry	Y	Y	Y
fs_rprt	Fail Soft Report	N	N	N
hol_entr	Holidays	Y	Y	Y
hol_rprt	Holidays	N	N	N
instentr	Instructions	Y	Y	Y
instrprt	Instructions	N	N	N
invtmenu	Key Inventory	N	N	N
job_entr	Jobcat	Y	Y	Y
job_rprt	Jobcat	N	N	N
josprprt	Special Journal Reporting	N	N	N
jourarch	Journal Archive	N	N	N
jourrprt	Journal Reporting	N	N	N
key_copy	Copy Keyholders	N	N	N
key_entr	Keyholders	Y	Y	Y
key_rprt	Keys Master	N	N	N
keyload1	Keyholder Loading Prog 1	N	N	N
ktimentr	Keyholder Timer Entry	Y	Y	Y
kyznrprt	Keyholder Zone	N	N	N
loadmenu	Key Holder Loading	N	N	N
loc_entr	Location	Y	Y	Y
loc_rprt	Location	N	N	N
lsumdel	Delete Lot Sum Records	N	N	N
lsumentr	Daily Lot Summary	Y	Y	Y
lsumrprt	Daily Lot Summary	N	N	N
mainmenu	SE / SMS Main Menu	N	N	N
mangrprt	Daily Manager's	N	N	N
maprprt	Maps	N	N	N
mealrprt	Meal Report	N	N	N
mlwkrprt	Hours vs. Meals Taken	N	N	N
mnaccopy	Copy Security	N	N	N
mod_pass	Modify Passwords	N	N	N
monitor	Monitor Security Activity	N	N	N
nodeentr	SE 422 Hardware Def	Y	Y	Y

outsrprt	Outstanding Tickets	N	N	N
overrprt	Tenant Overage	N	N	N
p422rprt	SE/422 PIN Report	N	N	N
padmmenu	Parking Administration	N	N	N
parkmenu	Parking Control	N	N	N
pgacentr	Security Entry	Y	Y	Y
pgacrprt	Security Master List	N	N	N
phstrprt	Point History	N	N	N
plotentr	Point/Lot Association	Y	Y	Y
pndfentr	SE422 PIN Definition	Y	Y	Y
pnt_entr	Points	Y	Y	Y
pnt_rprt	Points	N	N	N
pol_entr	Pollers	Y	Y	Y
pol_rprt	Pollers	N	N	N
prd_rprt	Project Reader Report	N	N	N
prj_entr	Project Definition	Y	Y	Y
prj_rprt	Project Report	N	N	N
psetmenu	Parking Setup	N	N	N
purgrprt	Purge A Pending Report	N	N	N
quckrprt	Quick Ticket Search	N	N	N
rdefentr	Device Report Definition	Y	Y	Y
rdefrprt	808 Report Definition	N	N	N
rdr_entr	Readers	Y	Y	Y
rdr_rprt	Readers	N	N	N
rpasrprt	Passback Zone Report	N	N	N
rprtmenu	Master File Reports	N	N	N
sec_menu	Program Security	N	N	N
sel_entr	Selection Table	Y	Y	Y
service	Ticket Servicing	N	N	N
showdate	Display Date & Time	N	N	N
showuser	Display All Valid Logins	N	N	N
showwho	Display All Users Logged In	N	N	N
siteentr	Site Entry Definition	Y	Y	Y
siterprt	Site Definition	N	N	N
spitentr	Ticket Spitter Synch	Y	Y	Y
statentr	Status Code Entry	Y	Y	Y
statmenu	Inventory Stat Code Menu	N	N	N
statrprt	Status Code Report	N	N	N
stkrentr	Parking Sticker Entry	Y	Y	Y
stkrmenu	Parking Stickers	N	N	N
stkrprt	Parking Sticker Master Rpt	N	N	N
stkrrprt	Parking Sticker Display	N	N	N
summdel	Delete Ticket Records	N	N	N
syclmenu	System Configuration	N	N	N
sys_menu	System Administration	N	N	N
taarch	Transaction Archiving	N	N	N
tacfentr	Conf Early / Late Hours	Y	Y	Y
taentr	Editing	Y	Y	Y
taexentr	T & A Exceptions	Y	Y	Y
tainrprt	Keyholder Inquiry	N	N	N
tarprprt	Detail / Summary Report	N	N	N
tartrprt	Offline Reporting	N	N	N
taskentr	Tasks	Y	Y	Y
taskrprt	Task / Event Master Report	N	N	N
tatransf	Record Transfer	N	N	N
tbleentr	Rate Tables	Y	Y	Y
tbllrprt	Tenant Billing	N	N	N
tententr	Tenants	Y	Y	Y
tentrprt	Tenants	N	N	N
termentr	Terminal / Point Xref	Y	Y	Y
thstrprt	Tour Schedule vs Access	N	N	N
tickentr	Ticket Editing	Y	Y	Y
tickpost	Post Serviced Tickets	N	N	N
tickrprt	Ticket Transaction Report	N	N	N
timemenu	Time & Attendance	N	N	N
tkeyrprt	Keyholder Tour History	N	N	N
tlogrprt	Ticket Log	N	N	N
tmcdentr	Time Codes	Y	Y	Y
tmcdrprt	Time Codes	N	N	N
tourmenu	Guard Tour	N	N	N
tranentr	Transactions	Y	Y	Y
trdsentr	Tour Definition	Y	Y	Y
trdsrprt	Tour Definition	N	N	N
trptmenu	Ticket Reports	N	N	N
trshentr	Tour Scheduling	Y	Y	Y
trshrprt	Tour Schedule	N	N	N
tsumrprt	Daily Ticket Summary	N	N	N
usraentr	Shift	Y	Y	Y
usrbentr	Emp Stat	Y	Y	Y
usrdmenu	User Defined Information	N	N	N
vctlentr	Badge Color Entry	Y	Y	Y
vistentr	Visitor Entry	Y	Y	Y
vistmenu	Visitors	N	N	N
vistrprt	Visitor Report	N	N	N
weekentr	Week Ending Dates	Y	Y	Y
whowhere	Passback Zone	N	N	N
zoneentr	Zones	Y	Y	Y
zonerprt	Zones	N	N	N

Level 2 = MONITOR ONLY

exit	Exit SE / SMS Application	N	N	N
mainmenu	SE / SMS Main Menu	N	N	N
monitor	Monitor Security Activity	N	N	N

INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

O

P

R

S

T

U

V

W

Y

Z