SECTION 1 - INTRODUCTION

1.1 STEPS FOR GETTING STARTED

1.1.1 How to Use this Manual

This manual is intended for both training and reference uses. It is divided into two parts. Part I covers installation and operation of your system and Part II covers maintenance troubleshooting and reference information. The Sections have been designed so that you can provide your employees with only the sections that are pertinent to them.

Front Desk Employees: We recommend the front desk employees receive copies of Section 2.2.1, Section 3 and Section 4 for instructions on using the equipment and handling Guest keys. Supervisors may need additional Sections depending on what they will be responsible for.

Housekeeping Employees: We recommend employees who will use master keys to clean rooms receive copies of Section 2.2.1 and Section 2.2.2 (if they will use Inhibit keys). Supervisors may need additional Sections depending on what they will be responsible for.

Initially, you should become familiar with each of the Part I sections. The Part II sections and Appendices can be used when needed. You should, however, familiarize yourself with what is in these sections by reviewing the Table of Contents.

1.1.2 Steps for Preparing for Your System Installation

This section lists all the steps you will need to take before and during installation in order to have a completely operational Saflok System. We recommend that you familiarize yourself with these areas of the manual and complete steps 1 through 7 before lock installation begins.

Step 1. When you receive your computer equipment, be sure to check the packing slips to make sure you have all the equipment. Then follow the steps in Section 1.3 SETTING UP THE STATION EQUIPMENT to set up all your equipment. Make sure you have also ordered keycards and determine how you will store your Failsafe keycards (see Section 6.1 Information on Failsafe Keys).

Step 2. Review the information you were sent on your Key Design to ensure that you are not missing any rooms and know how your master keys are designed. If your design is missing anything, it is important to contact your Saflok Technical Support office.

Step 3. Once your DeskLinc System is set up, you should immediately set the system date and time and DST information. You will have a fully authorized user with password 250 in the system. Refer to Section 3.1 through 3.3 to sign onto the Terminal and Sections 11.1 through 11.3 to set the system date & time and DST information. YOU MUST DO THIS BEFORE YOU MAKE KEYS OR PROGRAM LOCKS. If you have a Spare DeskLinc Terminal, you should also do this step for it.

Step 4. Determine who will need to use the Hand-Held Terminal(s) to make keys or program and interrogate locks and assign them user numbers and authorizations in the Terminal (refer to Section 7). If you have a Spare DeskLinc Terminal, you should also do this step for it.

Step 5. You should next train your staff on how to make keys. If you have a demonstration lock, you can program it to room DEMO or one of the training rooms from your key design (typically rooms 71 to 75 unless these are real rooms in your property). Your Front Desk personnel should learn how to use a key (Section 2), how to sign on and make keys (Section 3) and how to make guest keys (Section 4). Section 7 explains how to program a lock.

Step 6. You should next determine who will need master keys and make them. Refer to Section 5 MASTER KEYS and your Key Design for the keys to make. Once they are made, you should instruct your staff how to use them (Section 2). You should also determine who will need special keys - PPK, SPK, Status Keys and Display keys. Refer to Section 7 on how to make them and use them.

Step 7. You should next make your Failsafe keys. You can do this during or after lock installation, however, it is important to at least get a start on these keys. Refer to Section 6 FAILSAFE KEYS for information on how to make and store them. You should also set up your procedures for your staff to use them.

Step 8. As locks are installed, they should be programmed. Refer to Section 8.1 PROGRAMMING LOCKS for this procedure.

Step 9. You should also determine how your staff should handle keycard and lock calls and make sure they are trained in the procedures.

1.2 SYSTEM DESCRIPTION AND COMPONENTS

1.2.1 The DeskLinc System with Insertion Encoder

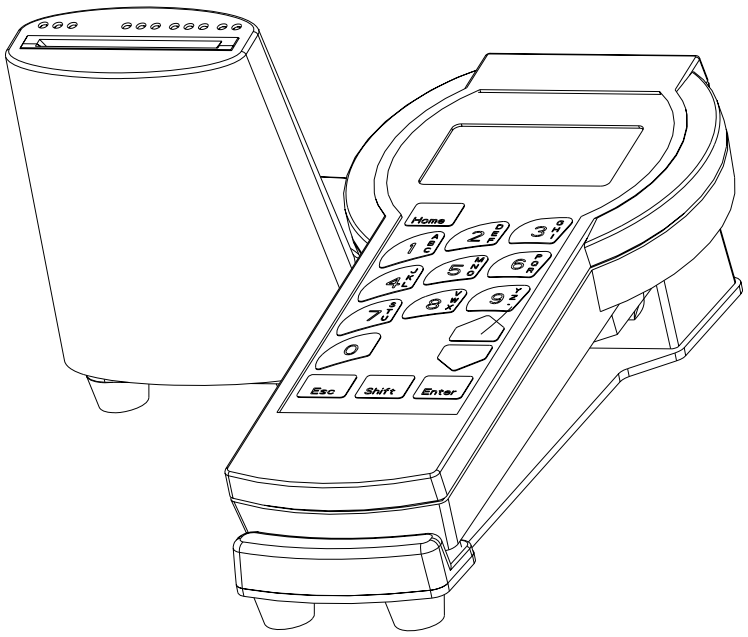
The basic DeskLinc System includes a Hand-Held DeskLinc Main Terminal, Insertion encoder, Saflok door locks, a Lock Programming & Interrogating/Emergency Lock Power Supply (LPI/ELPS) probe and magnetic-strip keys. A dot-matrix system printer is optional.

Hand-Held DeskLinc Main Terminal and Key Encoding Station
The Hand-Held DeskLinc Terminal contains all the key coding information, the key design (room and master key assignments), users and authorizations and transaction history. It is connected to a key encoder and can be used to make all guest, failsafe and master keys. An LPI/ELPS Probe can also be connected to the Terminal for programming, interrogating, and overriding low lock batteries.

Optional Printer
A dot-matrix parallel printer can be connected to the Hand-Held DeskLinc Terminal to print reports. A printer cable is included in the system even if the printer is not purchased.

Lock Programming & Interrogating / Emergency Lock Power Supply (LPI/ELPS) Probe
The Lock Programming & Interrogating / Emergency Lock Power Supply (LPI/ELPS) Probe serves as a communication interface between the Hand-Held Terminal and the lock. When a lock needs to be programmed or interrogated the LPI/ELPS Probe is connected to the Hand-Held Terminal and taken to the door. The LPI/ELPS Probe can also be connected to the Hand-Held Terminal and be used to open a lock that has a dead battery.

Magnetic Strip and Memory Keycards (Optional)
The magnetic strip keycard has a magnetic strip on it where the key coding information is stored. The memory keycard has a memory-chip where it stores the key coding information. Memory keys can also store key uses. Current available memory keycard sizes are 2Kbits, 8Kbits, and 64Kbits. The Saflok MT and Adese series locks are designed for reading both magnetic stripe and memory style keycards. Both keycards can be reused (re-encoded).



DeskLinc System

1.2.2 Other Optional Equipment

Custom Designed Keycards
Many customers prefer to use keycards designed for their property or hotel chain. If you would like a custom designed keycard, you can contact your Saflok representative for additional information and pricing.

Color Coded Master Keycards
Many customers prefer to use different colored keycards for their various master keys. There are four different standard colors available - Red, Blue, Yellow and Green. If you would like colored master keys, you can contact your Saflok representative for additional information and pricing.

Memory Keycards
Memory keycard are available for use with the DeskLinc system. The advantage of using these keys is that they will track where the key has been used. Many properties use these keys for the employee master keys. If you would memory keycards, you can contact your Saflok representative for additional information and pricing.

Guest Keycard Brochures
Many customers prefer to use Guest Keycard Brochures when they give keycards to a guest. The brochures have short instructions explaining how to use the keys, a place for the Room # to be written and a pocket to insert the keys. A generic brochure is available, however, you can also custom design a brochure. If you would more information or pricing on keycard brochures, you can contact your Saflok representative.

Failsafe Key Binders
Failsafe keys should be made for all the rooms in your property to allow you to issue guests new keys if you are unable to make keys on your Saflok System. One method for storing Failsafe keys is using loose-leaf binders with plastic pocket sheets for inserting the Failsafe keys for each room. Refer to the Failsafe Keys section of this manual for additional information.

Spare Hand-Held DeskLinc Computer Terminal
A spare DeskLinc Computer Terminal can be purchased to use for lock interrogations (instead of using the main DeskLinc Terminal) and to provide spare equipment that can be immediately put on line if the main DeskLinc Terminal becomes inoperable. It can be located anywhere and will require one power outlet.

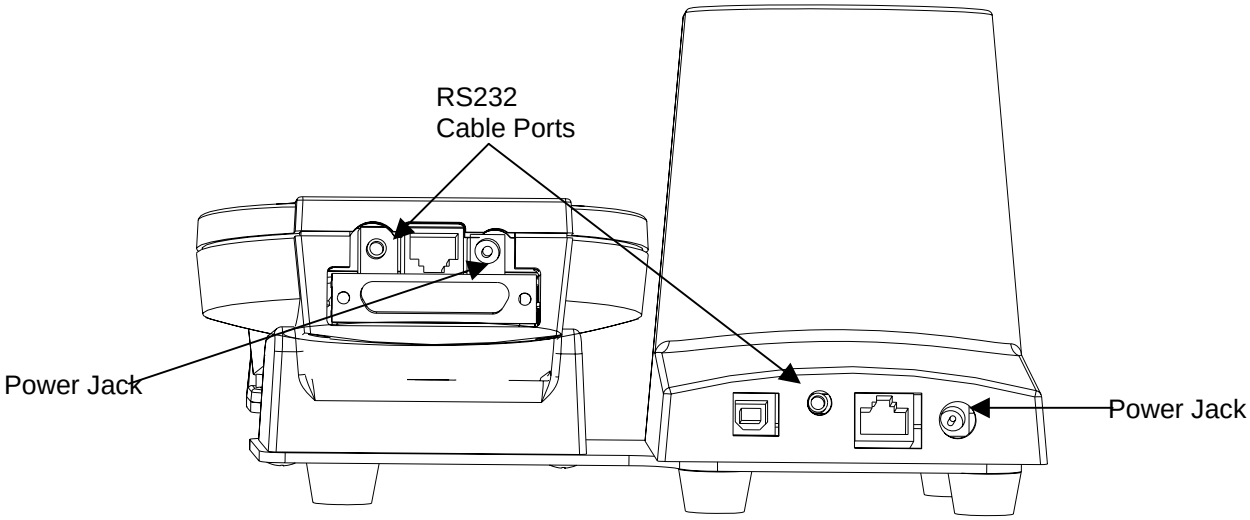
Hand-Held Front Desk LPI & Key Encoding Station
Up to 9 additional key making and LPI stations can be added to the DeskLinc System. These stations are designed for Front Desk use and will make guest keys. In addition, they can be used to program or interrogate locks. Each station consists of a Hand-Held Front Desk Terminal and a key encoder. It must be connected to the Hand-Held DeskLinc Station via an Ethernet Switch and category 5 cables.

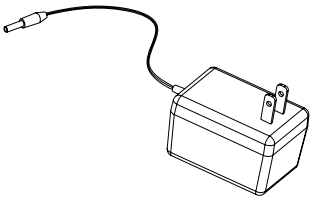
1.3 SETTING UP A SINGLE STATION SYSTEM

1.3.1 Setting Up the DeskLinc Key Making Station

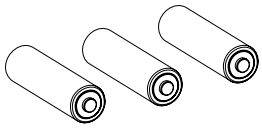
The Hand-Held DeskLinc Terminal Key Station is intended for use at Front Desk check in positions or the Front Office. It is designed to make all guest, failsafe and master keys and perform all the system maintenance functions and reports. It is also used for programming, interrogating and overriding low lock batteries. The station equipment consists of the following items:

- Hand-Held DeskLinc Terminal and power supply
- 3 NiMH Batteries for Hand-Held Terminal
- RS232 Cable to connect from Terminal to Encoder
- Insertion Encoder with base and power supply
- Printer Cable
- LPI/ELPS Probe & Cable

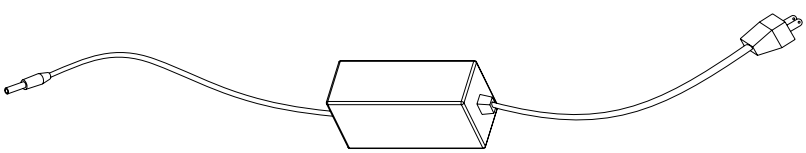




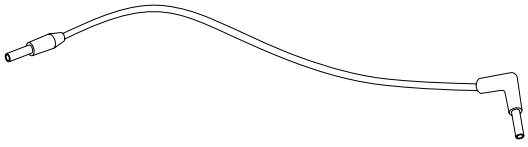
Insertion Encoder
Power Supply



NiMH Batteries



DeskLinc Terminal
Power Supply



RS232 Cable

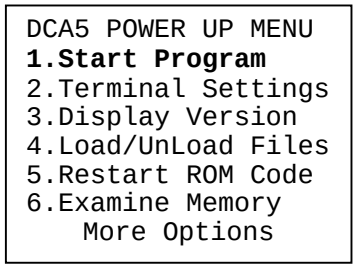
Step 1. Your Hand-Held should be shipped with all the batteries installed and a pull tab inserted in the battery case. If the tab is there, pull the tab out and discard it. The Terminal should then display a POWER UP MENU. If you were shipped separate batteries, remove the Hand-Held Terminal from the Base and open the battery cover. Insert the (3) batteries being careful to note the proper +/- directions (see Section 13.1). Replace the battery cover and reinsert the Terminal into the Base.

Step 2. Make sure the Hand-Held Terminal sits securely in the base.

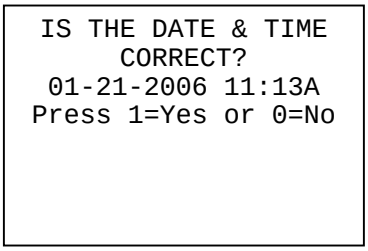
Step 3. Connect the RS232 Cable to the Encoder and the Hand Held Terminal. The thin 90-degree plug inserts into the top side of the Hand-Held Terminal the other end plugs into the back of the Encoder unit.

Step 4. Plug the Power Supplies for the Hand-Held Terminal and Encoder into the power jack on each then into a wall socket.

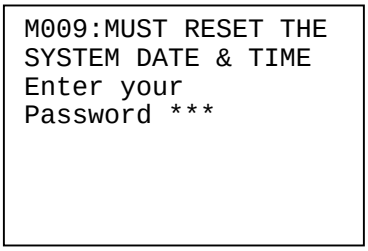
Step 5. Once the Terminal's batteries tab has been removed the Hand-Held Terminal it will display the POWER UP MENU screen.



To start the program, simply press ENTER. The terminal should display the following screen.



Step 6. If the date and time is correct, press 1 and then the terminal will display the password screen. If the date and time is not correct, press 0. If button 0 is pressed the terminal should display the following screen.



Step 7. Enter the default password 250 and then press ENTER. When screen on the left is displayed, press 1 to change the date and time. When the screen on the right is displayed input the date. Type the month then ENTER. Type the date then press ENTER, type the year then press ENTER.

```
SYSTEM DATE & TIME
01-21-06 11:45P DST
Change Date & Time?
Press 1=Yes or 0=No
```

```
001:ENTER NEW DATE
Month (1-12) 1
Date  (1-31) 21
Year         2006
```

Step 8. The DeskLinc computer will then go to the screen to enter the new time. Type the hour then press ENTER. Type the minutes then press ENTER. Type 0 for am or 1 for pm then press ENTER.

```
002:ENTER NEW TIME
Hour  (1-12) 11
Mins  (0-59) 45
AM (0) or PM (1)
```

Step 9. When the New Date & Time screen appears, confirm the date and time is correct. Press 1 for Yes. If 0 for No is selected you will return to step 6.

```
003:NEW DATE & TIME
01-21-06 11:45A DST
Is this Correct ?
Press 1=Yes or 0=No
```

Step 10. At the following screen press 1 for Yes to save the changes. The Password/Sign on screen will appear.

```
M220: Do You want to
Save the Changes

Press  1=Yes or 0=No
```

Step 11. If you have a system printer, use the Parallel Printer cable and follow the instructions in section 1.3.2. The remaining items you received with your system should be stored for future use.
- The encoder cleaning supplies
- The LPI/ELPS probe

1.3.2 Connecting a System Printer

The hand-held terminals are designed to work with a dot-matrix parallel printer. Although they may work with other types of printers, we cannot guarantee this. To connect a printer, follow these steps.

Step 1. Connect the 25 pin, D-shell connector end of the Parallel Printer Cable to the Terminal's printer port at the top of the Terminal. Connect the other end to the dot-matrix parallel printer.

Step 2. Make sure to plug your printer into power, turn it on and insert paper.

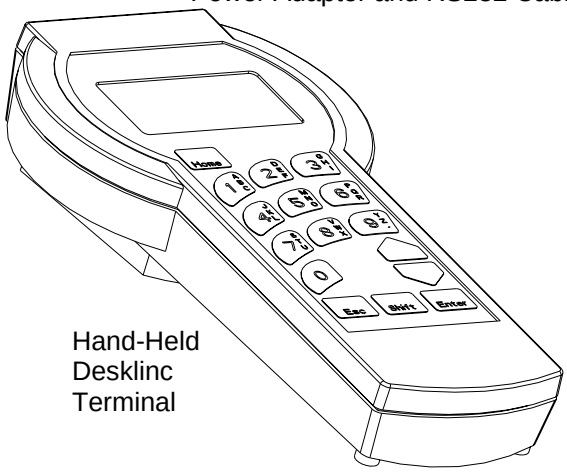
Step 3. To test your printer, you can do a PRINT SCREEN. To do a PRINT SCREEN, hold down the SHIFT key and press the Home key. Then release the keys. The printer should then print whatever the Terminal was displaying on its screen.

This will not work for printers that cannot accept a text dump and is not guaranteed to work with printers other than dot matrix. If the dot matrix parallel printer does not print, you should try the printer and the cable with other computers, printers or Hand-Held Terminals to identify which part is not working.

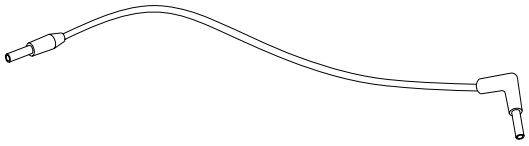
1.3.3 Setting Up a Spare DeskLinc Computer Terminal

A Spare DeskLinc Computer Terminal is intended for use if the main DeskLinc Computer Terminal becomes inoperable for any reason. It can also be used to interrogate locks instead of using the main DeskLinc Computer. The spare equipment consists of the following items:

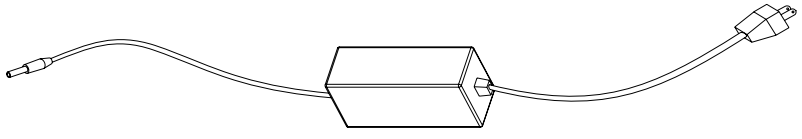
- Hand-Held DeskLinc Terminal and Power Supply
- 3 NiMH Batteries for Hand-Held Terminal
- Power Adapter and RS232 Cable



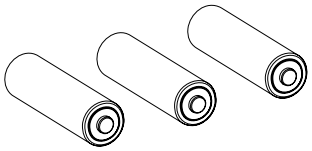
Hand-Held Desklinc Terminal



RS232 Cable



DeskLinc Terminal Power Supply



NiMH Batteries

Step 1. Your Hand-Held should be shipped with all the batteries installed and a pull tab inserted in the battery case. If the tab is there, pull the tab out and discard it. The Terminal should then display a POWER UP MENU. If you were shipped separate batteries, remove the Hand-Held Terminal from the Base and open battery cover. Insert the (3) batteries being careful to note the proper +/- directions (see Section 13.1). Replace the battery cover.

Step 2. Plug the Hand-Held Power Supply into the topside of the Hand-Held and a wall outlet.

Step 3. You may either store or connect the RS232 Cable. It is simply a spare cable. There is no Encoder to connect to the Terminal. If you wish to leave it connected to the Spare DeskLinc Terminal, the thin 90-degree plug inserts into the topside of the Hand-Held Terminal above the screen.

Step 4. Once the Terminal's batteries tab has been removed and the power supply is connect to a wall socket, it will display the POWER UP MENU screen.

```
DCA5 POWER UP MENU
1.Start Program
2.Terminal Settings
3.Display Version
4.Load/UnLoad Files
5.Restart ROM Code
6.Examine Memory
   More Options
```

To start the program, simply press ENTER. The terminal should display the following screen.

```
 IS THE DATE & TIME
     CORRECT?
 01-21-2006 11:13A
Press 1=Yes or 0=No
```

Step 5. If the date and time is correct, press 1 and then the terminal will display the password screen. If the date and time is not correct, press 0. If 0 for No is pressed the terminal should display the following screen.

```
M009:MUST RESET THE
SYSTEM DATE & TIME
Enter your
Password ***
```

Step 6. Enter the default password 250 and then press ENTER. When screen on the left is displayed, press 1 to change the date and time. When the screen on the right is displayed input the date. Type the month then ENTER. Type the date then press ENTER, type the year then press ENTER.

```
SYSTEM DATE & TIME
01-21-06 11:45P DST
Change Date & Time?
Press 1=Yes or 0=No
```

```
001:ENTER NEW DATE
Month (1-12) 1
Date  (1-31) 21
Year         2006
```

Step 7. The DeskLinc computer will then go to the screen to enter the new time. Type the hour then press ENTER. Type the minutes then press ENTER. Type 0 for am or 1 for pm then press ENTER.

```
002:ENTER NEW TIME
Hour  (1-12) 11
Date  (0-59) 45
AM (0) or PM (1)
```

Step 8. When the New Date & Time screen appears, confirm the date and time is correct. Press 1 for Yes. If 0 for No is selected you will return to step 6.

```
003:NEW DATE & TIME
01-21-06 11:45A DST
Is this Correct ?
Press 1=Yes or 0=No
```

Step 9. At the following screen press 1 for Yes to save the changes.

```
M220: Do You want to
Save the Changes

Press  1=Yes or 0=No
```

Step 10. The Password / Sign On screen should now appear and the terminal is ready to use. Since this is a spare DeskLinc Terminal and is not connected to the rest of your system, you will need to add users, passwords and authorizations (see Section 9).

1.4 SETTING UP A MULTI STATION SYSTEM

The Saflok DeskLinc system can be configured for multi-station encoding. Keycards can concurrently be encoded from up to 10 stations. Basic network typology consists of a Main station, Front Desk station, and Ethernet Switch. Each device within a station will require a Category 5 cable run to a switch for network conductivity. Please reference Figure-1 below to view the basic network layout.

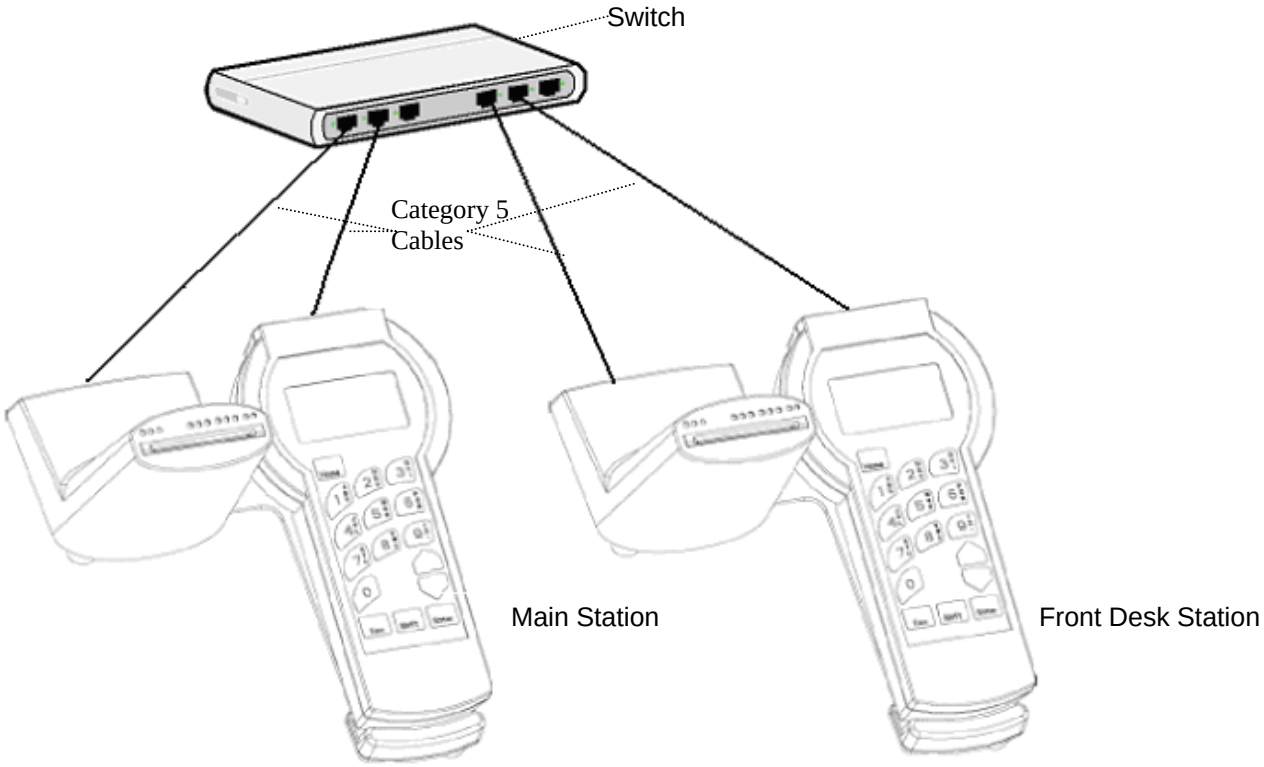


Figure 1

Basic Required Equipment:

- 1 Main DeskLinc Terminal w/ power supply
- 1 Main Encoder w/ power supply
- 1 Front Desk DeskLinc Terminal w/ power supply
- 1 Front Desk Encoder w/ power supply
- 4 Port Ethernet Switch or Hub w/power supply
- 4 Category 5 cables

1.4.1 DeskLinc Front Desk Station Network Configuration

Step 1. Connect the front desk station's terminal and encoder to the switch as illustrated in Figure-2 below.

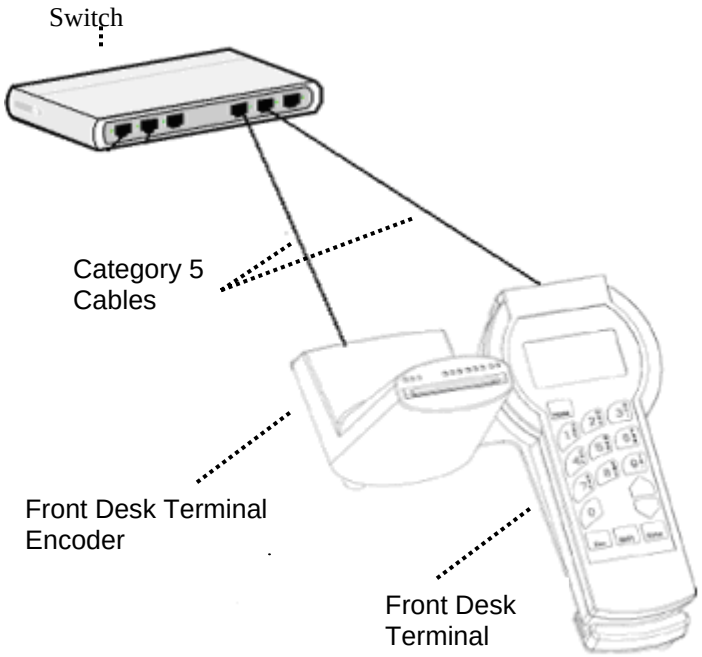


Figure-2

Step 2. Once the Front Desk Terminal's batteries tab has been removed and the power supplies are connected to a wall sockets for all devices, the Front Desk terminal will display the POWER UP MENU screen.

```
DFA5 POWER UP MENU
1.Start Program
2.Terminal Settings
3.Display Version
4.Load/UnLoad Files
```

Step 3. Press 2 or use the ARROW DOWN key to display the 2.Terminal Settings menu item. Press ENTER.

Step 4. At the TERMINAL SETTINGS screen press 2 or use the ARROW DOWN key to display the 2.Network Selection menu item. Press ENTER.

```
TERMINAL SETTINGS
1.Terminal Printer
2.Network Selection
3.LPI Probe Type

*** ESC to Exit ***
```

Step 5. Press 2 or use the ARROW DOWN key to display the 2.TCPIP Interface menu item. Press ENTER.

```
INTERFACE SETTINGS
1:RS232 Interface
2:TCPIP Interface

*** ESC to Exit ***
```

Step 6. The TCPIP INFO & SETTINGS screen will appear. Press Y to modify the settings. Press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-E4
MyIP: 0  .0  .0  .0
My Port:0
Station Num: 0

Modify Settings? Y
*** ESC to Exit ***
```

Step 7. The TCPIP INFO & SETTINGS edit screen will appear. Input a valid IP address next to MyIP, then press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-E4
MyIP: 192.168.1  .2
My Port:0
Station Num:0 (2-10)

*** ESC to Discard***
```

Step 8. The cursor will now move to My Port. Enter **5267** then press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-E4
MyIP: 192.168.1  .2
My Port:5267
Station Num:0 (2-10)

*** ESC to Discard***
```

Step 9. At the Station Num. field input a valid station number (start with station number 2 and increment from there for each additional station) then press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-E4
MyIP: 192.168.1  .2
My Port:5264
Station Num:2 (2-10)

*** ESC to Discard***
```

Step 10. The TCPIP ENCODER SETTINGS screen will appear. Press Y then ENTER on Scan for Encoder and Y then ENTER on Mod or Init Encoder.

```
TCPIP ENCDR SETTINGS
MAC:00-00-00-00-00-00
E-IP: 0  .0  .0  .0
Encdr PMS Port: 0

Scan for Encoder?Y
Mod or Init Encoder?Y
*** ESC to Exit ***
```

Step 11. After the scan for network encoders is completed the first encoder found will be displayed on the SELECT ENCODER screen. Look at the MAC Address on the bottom of the encoder. If the MAC Address of the encoder displayed on screen matches the MAC address on the bottom of the encoder, press Y then ENTER. If not, press N then ENTER to display the next encoder found, then repeat this step until the correct encoder is selected.

```
SELECT ENCODER
MAC:00-0E-2A-80-03-46
E-IP: 0  .0  .0  .0
Port:5264
Ver02/14/2005-16
Select this Encdr?Y

*** ESC to Exit ***
```

Step 12. The TCPIP ENCDR SETTINGS screen will appear. Next to E-IP type in a valid encoder IP address then press ENTER.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-46
E-IP: 192.168.1  .4
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 13. The cursor will now move to Encdr PMS Port field. Enter **5264** then press ENTER.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-46
E-IP: 192.168.1  .4
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 14. Enter Y to initialize the encoder. Then press ENTER. This process assigns the displayed encoder to the front desk terminal.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-46
E-IP: 192.168.1  .4
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 15. The terminal will return to the TERMINAL SETTINGS screen. Press ESC.

```
TERMINAL SETTINGS
1.Terminal Printer
2.Network Selection
3.LPI Probe Type

*** ESC to Exit ***
```

Step 16. The POWER UP MENU screen will appear. The front desk station is now configured. Allow the terminal to stay on this screen until the main station has been configured and displays the password screen.

```
DFA5 POWER UP MENU
1.Start Program
2.Terminal Settings
3.Display Version
4.Load/UnLoad Files
```

Step 17. Proceed to the DeskLinc Main Station Network Configuration (Section1.4.2).

1.4.2 DeskLinc Main Station Network Configuration

Step 1. Connect the main station's hand held terminal and encoder to the switch as illustrated in Figure-3 below.

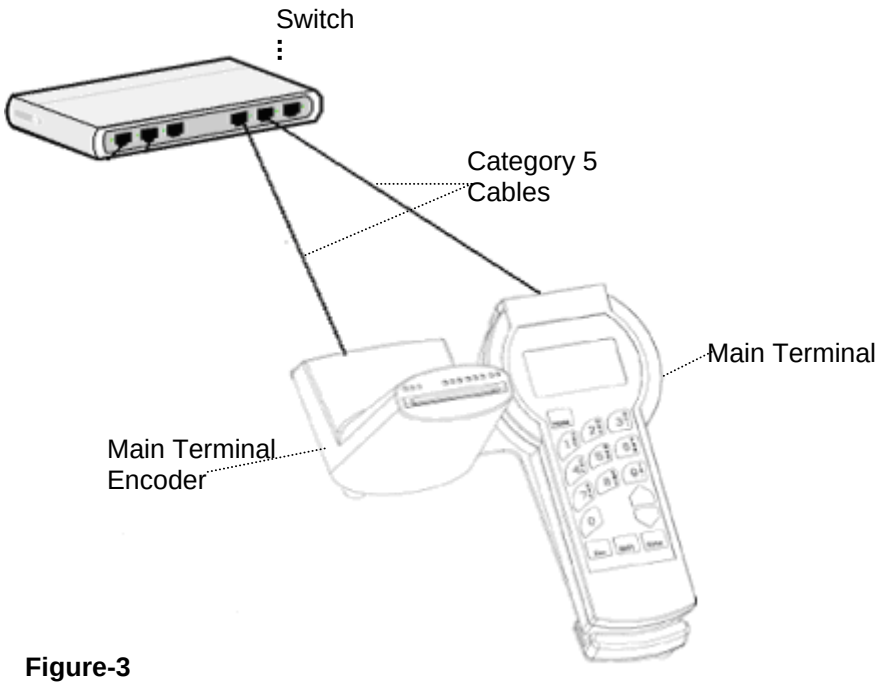


Figure-3

Step 2. Once the Main Terminal's batteries tab has been removed and the power supplies are connected to a wall sockets for all devices, the main terminal will display the POWER UP MENU screen.

```
DCA5 POWER UP MENU
1.Start Program
2.Terminal Settings
3.Display Version
4.Load/UnLoad Files
5.Restart ROM Code

    More Options
```

Step 3. Press 2 or use the ARROW DOWN key to display 2.Terminal Settings menu item. Press ENTER.

Step 4. Press 2 or use the ARROW DOWN key to display the 2.Network Selection menu item. Press ENTER.

```
TERMINAL SETTINGS
1.Terminal Printer
2.Network Selection
3.LPI Probe Type

*** ESC to Exit ***
```

Step 5. Press 2 or use the ARROW DOWN key to display the 2.TCPIP Interface menu item. Press ENTER.

```
INTERFACE SETTINGS
1.RS232 Interface
2.TCPIP Interface

*** ESC to Exit ***
```

Step 6. The TCPIP INFO & SETTINGS screen will appear. Press Y to modify the settings. Press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-FA
MyIP: 0  .0  .0  .0
My Port:0
GtWy: 0  .0  .0  .0
SbNt: 0  .0  .0  .0
Modify Settings? Y
*** ESC to Exit ***
```

Step 7. The TCPIP INFO & SETTINGS edit screen will appear. Input a valid IP address next MyIP then press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-FA
MyIP: 192.168.1  .1
My Port:0
GtWy: 0  .0  .0  .0
SbNt: 0  .0  .0  .0

*** ESC to Discard***
```

Step 8. In the My Port field input value **8264**. Press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-FA
MyIP: 192.168.1  .1
My Port:8264
GtWy: 0  .0  .0  .0
SbNt: 0  .0  .0  .0

*** ESC to Discard***
```

Step 9. Next to GtWy input a valid network gateway IP address. Press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-FA
MyIP: 192.168.1  .1
My Port:43266
GtWy: 192.168.2  .1
SbNt: 0 .0  .0  .0

*** ESC to Discard
***
```

Step 10. Input a valid subnet IP address next to SbNt. Press ENTER.

```
TCPIP INFO & SETTINGS
MAC:00-60-35-04-A1-FA
MyIP: 192.168.1  .1
My Port:43266
GtWy: 192.168.2  .1
SbNt: 255.255.0  .0

*** ESC to Discard
***
```

Step 11. The TCPIP ENCODER SETTINGS screen will appear. Press Y then ENTER on Scan for Encoder and Y then ENTER on Mod or Init Encoder.

```
TCPIP ENCDR SETTINGS
MAC:00-00-00-00-00-00
E-IP: 0  .0  .0  .0
Encdr PMS Port: 0

Scan for Encoder?Y
Mod or Init Encoder?Y
*** ESC to Exit ***
```

Step 12. After the scan for network encoders is completed the first encoder found will be displayed on the SELECT ENCODER screen. Look at the MAC Address on the bottom of the encoder. If the MAC Address of the encoder displayed on screen matches the MAC address on the bottom of the encoder, press Y then ENTER. If not, press N then ENTER to display the next encoder found, then repeat this step until the correct encoder is selected.

```
SELECT ENCODER
MAC:00-0E-2A-80-03-48
E-IP: 0  .0  .0  .0
Port:5264
Ver02/14/2005-16
Select this Encdr?Y

*** ESC to Exit ***
```

Step 13. The TCPIP ENCDR SETTINGS screen will appear. Input a valid encoder IP address next to E- IP. Press ENTER.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-48
E-IP: 192.168.1  .3
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 14. Next to Encdr PMS Port input value **5264**. Press ENTER.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-48
E-IP: 192.168.1  .3
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 15. Enter Y to initialize the encoder. Press ENTER. This process assigns the displayed encoder to the main terminal.

```
TCPIP ENCDR SETTINGS
MAC:00-0E-2A-80-03-48
E-IP: 192.168.1  .4
Encdr PMS Port: 5264

Initialize Encoder? Y
*** ESC to Exit ***
```

Step 16. The TCPIP SLAVE SETTINGS screen will appear. Press Y then ENTER on both Scan for Slaves and Display Slaves.

```
TCPIP SLAVES SETTINGS
There are currently
00 stations defined

Scan for Slaves? Y
Display Slaves? Y

*** ESC to Exit ***
```

Step 17. After the scan for slave (Front Desk) terminals is completed the first terminal will be displayed on the VALIDATE STATION screen.
If the information is correct for the station information displayed, press N then ENTER on Mod or Send Settings .
If the information is not correct, press Y then ENTER on Mod or Send Settings and the second screen below will display. At this screen you can modify the information. Then Press Y then ENTER on Send Current Setting.

```
VALIDATE STATION 2
MAC:00-60-35-04-A1-FC
IP:     192.168.1.2
Port:      5267
Ver: FD5-04/15/06.0

Mod or Send Settings N
*** ESC to Exit ***
```

```
VALIDATE STATION 2
MAC:00-60-35-04-A1-FC
IP:     192.168.1.2
Port:      5267
Ver: FD5-04/15/06.0

Send current setting Y
*** ESC to Exit ***
```

Note: If additional Front Desk terminals need to be validated, repeat this step.

Step 18. Press ESC. The terminal will return to the TERMINAL SETTINGS menu screen. Press ESC again to get to the POWER UP Menu. All stations are configured after this point.

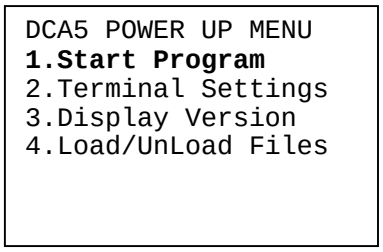
```
TERMINAL SETTINGS
1.Terminal Printer
2.Network Selection
3.LPI Probe Type

*** ESC to Exit ***
```

Step 19. Proceed to the Putting the DeskLinc System Online section.

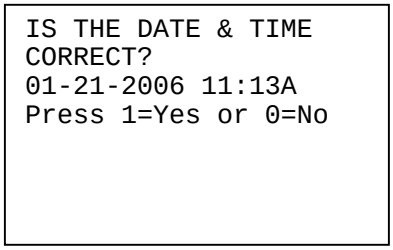
```
DCA5 POWER UP MENU
1.Start Program
2.Terminal Settings
3.Display Version
4.Load/UnLoad Files
```

1.4.3 Putting the Multi Station System Online

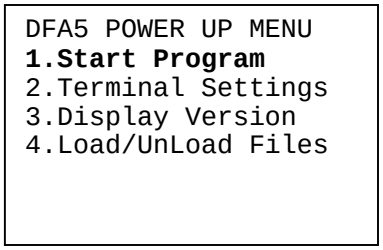
Step 1. With main terminal at the POWER UP MENU Press 1 or use the ARROW DOWN key to display the 1. Start Program menu item. Press ENTER.



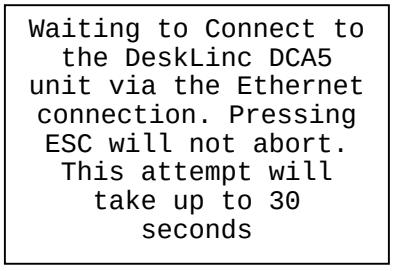
Step 2. Press 1 for Yes if the date and time is correct. The main terminal will go to the Password screen. Press 0 for No to correct the date and time (see Section 1.3.1 for details on setting the date and time in the terminal).



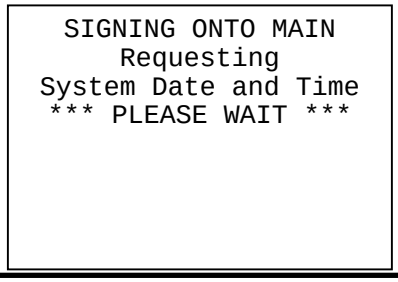
Step 3. Once the Main terminal is on the Password screen, with the Front Desk terminal at the POWER UP MENU press ENTER on 1. Start Program menu item to start the link process to the main terminal.



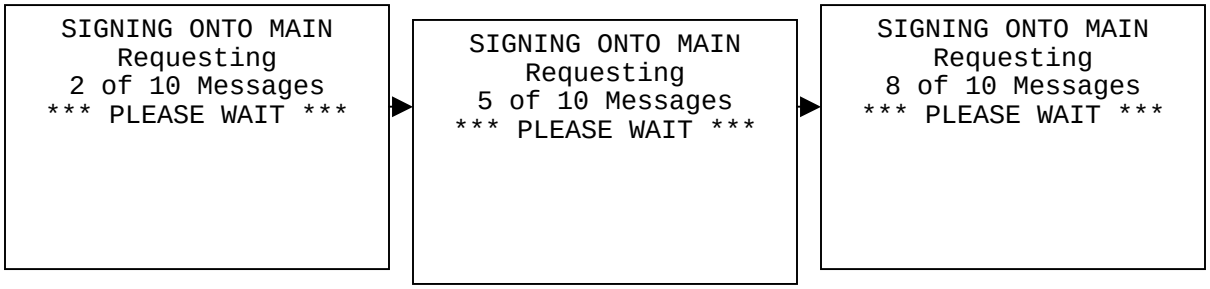
Link Process 1: The following screen will briefly display.



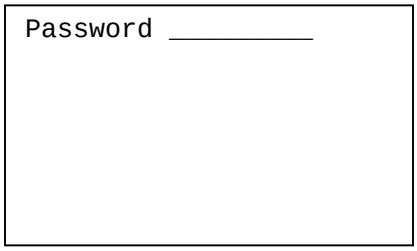
Link Process 2: The Front Desk terminal will proceed to request the date and time from the main terminal.



Link Process 3: After Link Process 2 has completed the Front Desk terminal will proceed to receive up to 10 link messages.



Step 4. When all link messages have been received, the Front Desk terminal will go to the Password screen. The Front Desk terminal and Main terminal are now online and ready to perform transactions.



SECTION 2 - LOCK & KEYCARD OPERATION

2.1 LOCK AND KEYCARD FEATURES

2.1.1 Lock Features

LOCK LEVELS: Each lock can be programmed for up to 12 different key or lock levels (10 for access keys and 2 for programming). Guest room locks and Special door locks are typically programmed differently.

GUEST ROOM LOCK LEVELS

Room Level - These keys will only open one lock and are issued to Guests.
Suite Level - These keys will typically open several rooms with connecting doors and are also issued to Guests.
Limited-Use Level – These keys will open one lock 2 times or until its specified number of days at 11:59pm, whichever comes first.
Failsafe Level - These keys only open one lock. They are pre-made and issued to new Guests if keys cannot be made at the Saflok System.
Section Level - These keys operate in a group of rooms and are intended for use by Housekeeping.
Floor Level - These keys typically operate all the rooms on a floor and are intended for use by Housekeeping inspectors.
Inhibit Level - These keys typically operate all the rooms in the property and are intended for use by Housekeeping inspectors. They will inhibit any the guest keys currently working in a lock and would be used after a guest has checked out. They do not open doors when they are used and will still inhibit guest keys if the dead bolt or privacy switch is activated.
Grand Master Level - These keys typically operate all the rooms in the property.
Security/Emergency Level- These keys typically operate all the rooms in the property and will override a dead bolt or privacy switch.
Electronic Lockout Level - These keys typically operate all the rooms in the property. They will electronically lock a lock from outside, preventing all keycards except the Security/Emergency key from entering a room. They do not open doors when they are used.
Secondary Program Key (SPK) Level - This key works in all the rooms in a property. It will not open a door and is used with other Special keys for troubleshooting.
Primary Program Key (PPK) Level - This key works in all the rooms in a property. It will not open a door and is used with other Special keys for troubleshooting.

SPECIAL LOCK LEVELS

Special locks include pass doors, elevators, meeting rooms, etc. Their levels are the same as for Guest Room locks except they have the following additional capabilities.

Pass Levels - The Room, Suite, Limited-Use, Failsafe, Section, Floor and Grand Master levels can be programmed as pass levels which will allow all the keys from the level to operate the lock. The Pass levels can also be designed so only specific pre-defined Room, Suite, etc. keys with a specific pass # will operate the lock.

Latch/Unlatch Level - These keys can be designed to operate an individual lock or a group of locks. When they are used, they will alternately leave the lock latched or unlatched. When a lock is unlatched, no keys are need to turn the door handle.

LOCK FEATURES

ELECTRONIC LOCKOUT

A lock can be electronically locked so that only the Security/Emergency key can open the door. This is done by using an Electronic Lockout key from outside the door. The key will toggle between locking and unlocking the door each time it is used. When a door is electronically locked, the other key levels would simply get a flashing yellow light.

INTERNAL CLOCK AND CALENDAR

The lock contains a clock crystal that maintains actual date and time. The time is updated every minute and the lock automatically adjusts the time and date for changes due to Daylight Savings Time and Leap Years. When valid keycards are used in the lock, the lock records the date and time from its clock. When locks are interrogated or programmed, their clock date and time is automatically updated.

PASS FEATURE: This feature is available for special locks such as entrance doors, pool doors, elevators or limited access doors. These locks would have the selected levels programmed with one or both of the following pass features.

- Automatic pass – keys are automatically allowed access during key encoding process
- Selectable pass – keys are selected to gain access during key encoding process

The levels that can be assigned the Pass feature include the Room, Suite, Limited-Use, Failsafe, Section, Floor and Grand Master levels. The automatic locks and keycards would need to be set up with the pass feature when your Key Design is created. Up to six different selectable pass areas can be assigned to a lock and key. A common use for the selectable feature would be VIP guest keys that should have access to a lounge or other areas while the regular guest keys should not.

All Pass: A level set up with All Pass, will allow all keys made for the level to operate the lock.

INVALID KEYCARD SHUTDOWN: This lock feature is designed to provide added security so a person cannot take a number of miscellaneous keycards to a lock in the chance one will work. If 10 invalid keys are used in the lock in a row, the lock will automatically shutdown for 1-2 minutes. If additional keys are used during this period, the lock will not display any lights and will not operate. After 1-2 minutes, if another invalid key is used, the 2 minute shutdown cycle will occur again. The use of a valid master key during the 1-2 minute shutdown cycle or the use of a valid key after 1-2 minutes will deactivate this feature.

LED DIAGNOSTICS: If a keycard does not work in a lock, the lock's LED diagnostic feature can be turned on to determine exactly why the key did not work. After LED diagnostics is turned on, the keycard that did not work can be used again. The lock will then display an error code using its lights which indicates why the key did not work. If the key was working normally, the lock will instead display the normal flashing green lights.

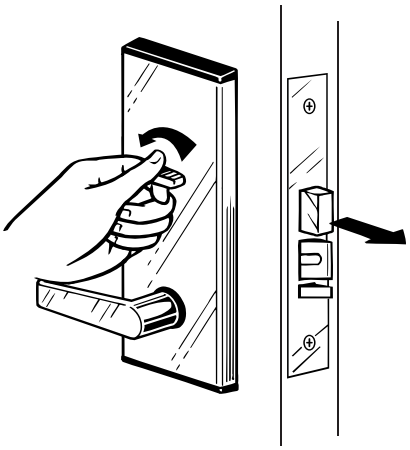
LOW BATTERY AND CLOCK NEEDS RESET INDICATIONS: The lock is designed to provide indications that its batteries are low and need replacing or its clock date & time need updating. Every guest and master key will display a red light with the normal lights when either of these lock conditions occurs. The Section and Floor keys will however work slightly differently. These keys have a "hassle" feature associated with them. The first time the key is used, ONLY the red light will flash and the door cannot be opened. If the key is used again, it will then get the red light with the normal lights and be able to open the door. The hassle feature is intended to prompt housekeeping to report locks that need batteries changed or clocks reset. Once this is done, the keys will all go back to operating normally.

AUTOMATIC UNLATCH/LATCH

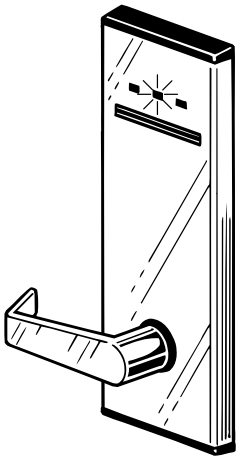
A lock can be programmed to automatically unlatch and latch at specified times for each day of the week. A keycard is not required to perform the unlatching and latching activities. When a lock is unlatched, no keycard is required to open the door. Locks with this feature must be configured in the design.

DEAD BOLT AND PANIC FEATURE (FOR LOCKS WITH STANDARD DEAD BOLT)
The SAFLOK MT and Adese series versions with standard dead bolts have this feature.

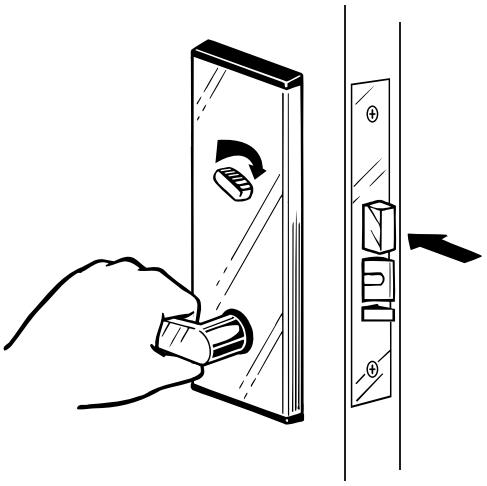
The dead bolt can be activated from inside the room by turning the dead bolt latch to the locked position.



When the dead bolt is activated, keycards that cannot override a dead bolt will get a flashing yellow light and will not be able to open the door. The Security/Emergency key and any guest keys that are programmed to override a dead bolt will get the normal flashing green light instead and will be able to open the door.

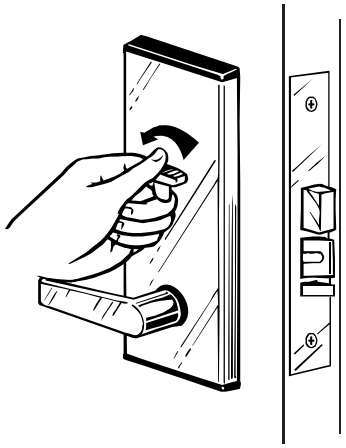


The "Panic" feature allows the dead bolt to be retracted from inside the room by simply turning the door handle. With this feature, there is no need to first turn the dead bolt latch to the unlatched position.

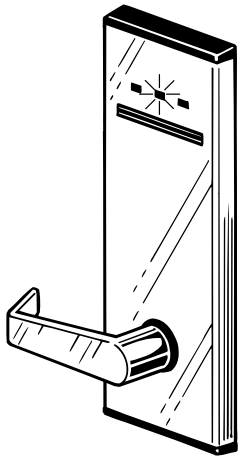


PRIVACY SWITCH AND PANIC FEATURE (FOR ADB MORTISE LOCKS):
The SAFLOK MT and Adese series ADB (automatic dead bolt) locks have this feature.

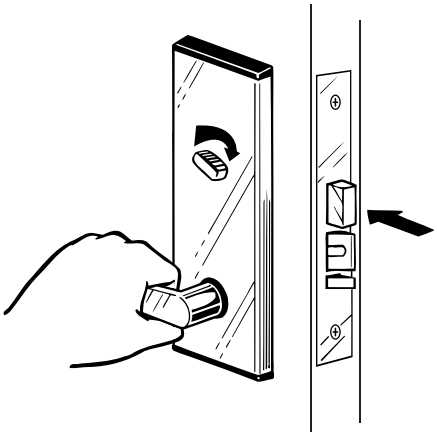
The Privacy feature can be activated from inside the room by turning the Privacy switch.



When the Privacy feature is activated, keycards that cannot override a dead bolt or privacy switch will get a flashing yellow light and will not be able to open the door. The Security/Emergency key and any guest keys that are programmed to override a dead bolt or privacy switch will get the normal flashing green light instead and will be able to open the door.



The "Panic" feature allows the Privacy switch to be deactivated from inside the room by simply turning the door handle.



2.1.2 Keycard Features

TYPES OF KEYCARDS:
There are two basic types of keycards. The keycards you make and issue for guest and master keys are Standard Keycards. The remaining types of keys are used for troubleshooting or maintenance and are referred to as Special Keys.

Standard Keys - These keys include all the normal guest, limited-use, failsafe and master keys that you make and issue. Sections 4, 5 and 6 cover how these keys work and how to make them.

Special Keys - These keys include the programming keys (PPK and SPK), the change Status keys (E2 Erase & LED Diagnostics), the Display keys and the Starter keys. Refer to Section 7 for details on how these keys work and how to use them.

KEYCARD SEQUENCES AND SKIPPING SEQUENCES: New keys are considered a new sequence of keys. When you make and use New keys, they will automatically cancel any previously issued keys for that key that were working in the lock. Except for guest keys, a new key for one level will not affect the keys working on the other levels. For instance a New Section #11 key will cancel any previously issued Section #11 keys, but it will not affect any Room, Floor, etc. keys and it will not affect another Section key (such as Section #12).

The locks will always accept the newest keys made from the Saflok System. In effect, you can make an unlimited number of new keys and not use them and the lock will still accept the next new key you make.

AUTOMATIC GUEST KEYCARD INHIBITING: When you make and use a New Guest key (Room, Suite or Failsafe), it will also automatically inhibit any other guest level key (Room, Suite or Failsafe) that was working in the lock. This ensures that there will only be one working guest level key in a lock at any one time.

OVERRIDE DEAD BOLT OR PRIVACY SWITCH: Typically only the Security/Emergency key can override a dead bolt or privacy switch to open a door. The other key levels would simply get a flashing yellow light. It is, however, possible to set up your Key Design to allow guest keys to override a dead bolt or privacy switch. If this is done, once a guest key was used, it would get the normal flashing green lights and be able to open the door. A New guest key would NOT be accepted and would NOT override a dead bolt. If the room is occupied and a new guest is mistakenly checked into the room, their new keeps will not cancel the current guest's key and will not override the dead bolt/privacy switch.

KEYCARD EXPIRATION: All the keycards are set up so they will expire, or stop working in the locks, after a certain date and time. Each keycard's expiration is set when the key is made.

For Guest keys, the key expiration will be a given number of days after the checkout date. When guest keys are made, the # of days until checkout is entered. The additional days for expiration is then added to this. The # of days for guest key expiration is set up in your Key Design (refer to Section 15.2.2 to view this information or 10.4 to request Report 1 of your Key Design).

For Failsafe keys, the keys will work for a given number of days from the time they are actually used in the lock. The number of days chosen by your property is also in the Key Design (refer to Section 15.2.2 to view this information or 10.4 to request Report 1 of your Key Design).

For Limited Use keys, the expiration will be based upon the number of days entered when the key is made. The key will work in the lock two times or until it's specified number of days at 11:59p.m., whichever comes first.

For Master keys, the # of days a key should work before expiring is entered when you make the keys. You can select a different key expiration for every key if you desire.

KEYCARD EXPIRATION WARNING: When a master key is getting close to its key expiration date, the lock will provide a warning light when the key is used. A single Yellow light will flash once before the green or yellow light flashes. This will begin to occur 7 days before the key actually expires. You should replace the key before it actually expires.

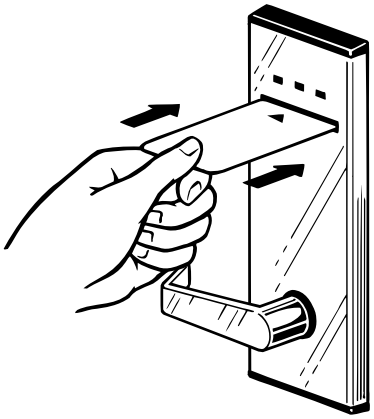
SHIFT TIMES: Masters level keys, except the emergency level, can be programmed to work only during certain shift hours of the day. When the keys is made the user can specify the start and end times of the shift. A key can only have one shift time specified. If the key is used outside the shift time it will not work.

2.2 USING KEYCARDS IN A LOCK

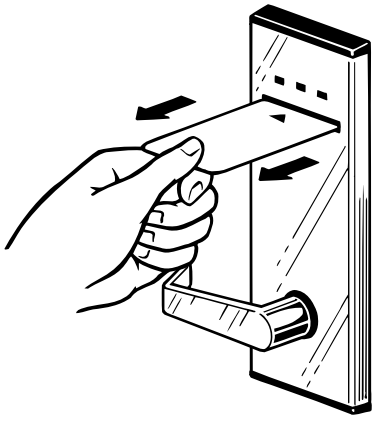
2.2.1 How to Use a Keycard in a Lock

Magnetic Keycards
The magnetic strip on the back of each key contains the key code information. The key must be inserted properly into the lock so this information can be read. All levels of keycards are used in this manner, however, different light patterns can occur when using keys. Refer to Section 2.3 for more information on what the different lock lights mean.

Step 1. Insert the keycard into the lock with the magnetic strip facing down and the arrows on the key pointing into the lock.



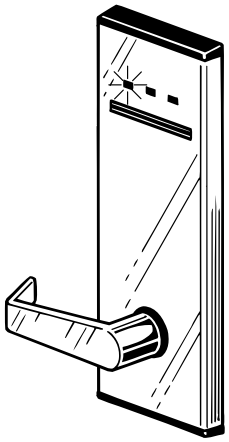
Step 2. Remove the keycard as soon as it has been fully inserted. The lock will not operate until the key has been withdrawn.



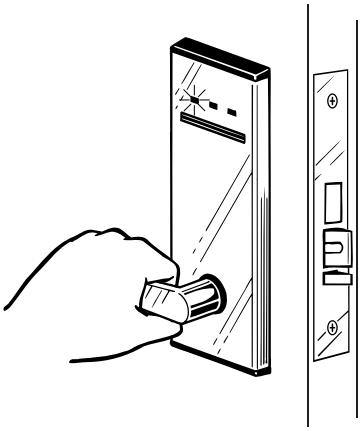
Step 3. If the door can be opened, a flashing green light will appear on the front of the lock as soon as the key is removed. It will flash for up to 6 seconds.

If you are using an Inhibit or an Electronic Lockout key, the yellow light will flash and may be preceded by a red flash instead. If you are using a Latch/Unlatch key, the green flashing light may be preceded by a red flash. Refer to Sections 2.2.2, 2.2.3 and 2.2.4 for explanations of these keys.

If other lights flash, refer to Section 2.3 for explanations.

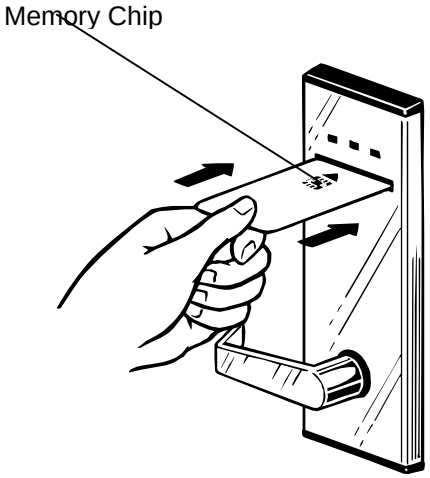


Step 4. While the green light is flashing, turn the handle to open the door. If the handle is not turned while the light is flashing, the lock will automatically re-lock.

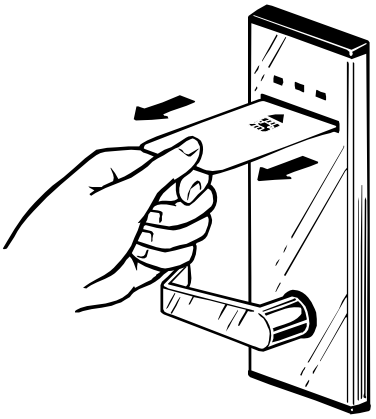


Memory Keycards

The memory-chip on the top of each key contains the key code information. The key must be inserted properly into the lock so this information can be read. All the keycards are used in this manner, however, different light patterns can occur when using keys. Refer to Section 2.3 for more information on what the different lock lights mean.



Step 1. Insert the keycard into the lock with the Memory chip facing up.

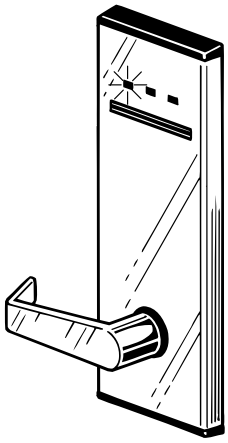


Step 2. Remove the keycard as soon as the green light flashed one time.

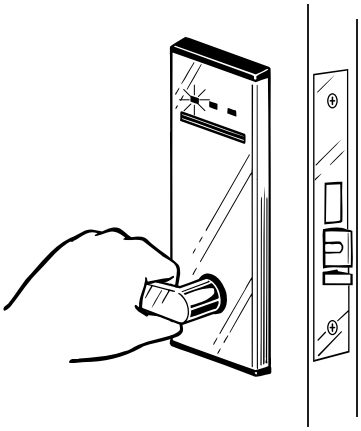
Step 3. If the door can be opened, a flashing green light will appear on the front of the lock as soon as the key is removed. It will flash for up to 6 seconds.

If you are using an Inhibit or an Electronic Lockout key, the yellow light will flash and may be preceded by a red flash instead. If you are using a Latch/Unlatch key, the green flashing light may be preceded by a red flash. Refer to Sections 2.2.2, 2.2.3 and 2.2.4 for explanations of these keys.

If other lights flash, refer to Section 2.3 for explanations.



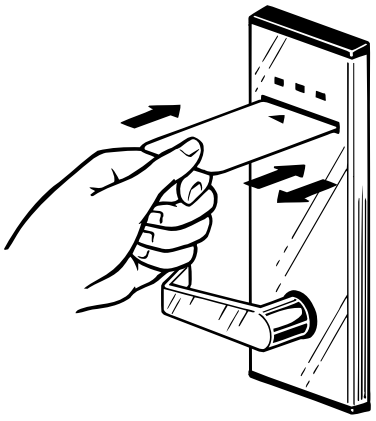
Step 4. While the green light is flashing, turn the handle to open the door. If the handle is not turned while the light is flashing, the lock will automatically re-lock.



2.2.2 Using an Inhibit Key in a Lock

The Inhibit key affects the guest level keys: Room, Suite and Failsafe. It inhibits the current sequence of key for each of these levels so that no previously issued guest key will operate the lock. The purpose is to prevent guests who have checked out from later re-entering the room if their keycard has not expired. It is generally used after the room has been cleaned and is ready for the next guest.

Step 1. Insert and remove the keycard in the lock.

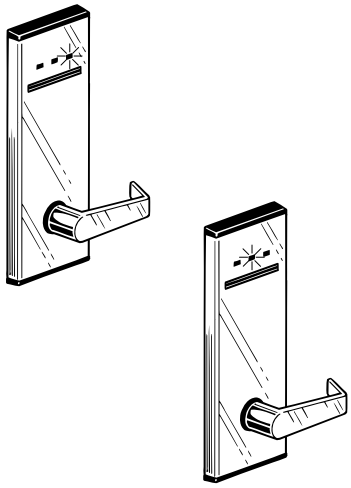


Step 2. The Inhibit key will not open the door. One of the two following light patterns should occur, indicating the key worked:

- One Red Flash followed by Flashing Yellow Lights (12 times) indicates that the guest keys were inhibited.

- Flashing Yellow Lights (12 times) indicate that the guest keys have already been inhibited.

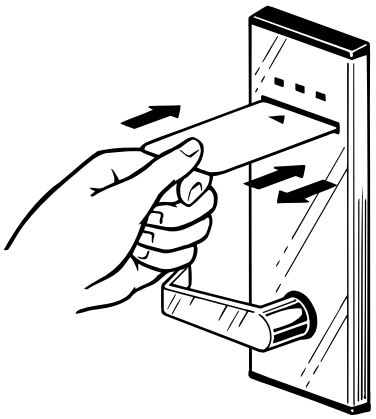
If other lights flash, refer to Section 2.3 for explanations.



2.2.3 Using an Electronic Lockout Key in a Lock

The Electronic Lockout key affects all the other key levels except the Security/Emergency key. It is used to electronically lock the door from outside the room so that only the Security/Emergency key can be used to open the door. The key will alternately lock and unlock the door each time it is used. When the lockout is activated, the current keys for the other levels will produce fast flashing yellow lights (8 times). The Security/Emergency key will still produce the normal green flashing lights and allow the door to be opened. When the Electronic Lockout key is used again to remove the lockout, the keys will again work normally.

Step 1. Insert and remove the keycard in the lock.

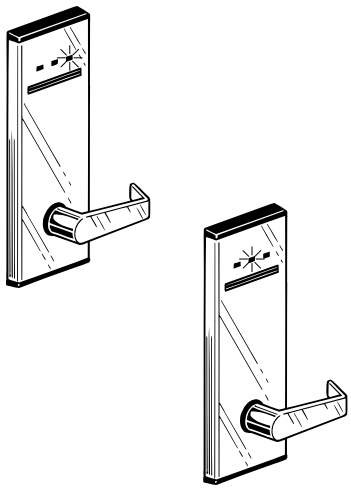


Step 2. The Electronic Lockout key will not open the door. One of the two following light patterns should occur, indicating the key worked:

- One Red Flash followed by Flashing Yellow Lights (12 times) indicates that the lock has been electronically locked.

- One Green Flash followed by Flashing Yellow Lights (12 times) indicate that the electronic lockout has been removed.

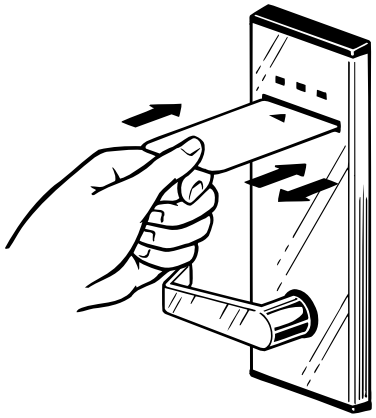
If other lights flash, refer to Section 2.3 for explanations.



2.2.4 Using a Latch/Unlatch Key in a Lock

The Latch/Unlatch key is intended to be used for entrance doors or meeting room type applications that do not have dead bolts or privacy. Guest rooms do not have these keys. The Latch/Unlatch key will alternately latch and unlatch the door each time it is used. When the door is left unlatched, no key is needed in order to turn the handle and open the door. The current keys for the other levels will continue to work normally, even though it is unnecessary to use them to open the door. Using an Electronic Lockout key (or the dead bolt or privacy switch) will NOT keep people from entering an unlatched lock - the lock must first be re-latched with the Latch/Unlatch key. When the Latch/Unlatch key is used to re-latch the door, the lock again works normally and requires keycards in order to open the door.

Step 1. Insert and remove the keycard in the lock.

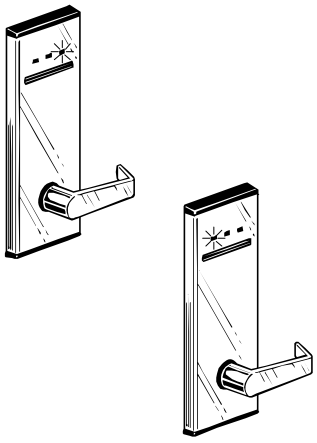


Step 2. The Latch/Unlatch key will always allow the door to be opened when it is used. Depending on the lights it gives, the door will be left latched or unlatched. One of the two following light patterns should occur, indicating the key worked:

- One Red Flash followed by Flashing Green Lights (12 times) indicates that the lock has been re-latched and will re-lock when the lights go out.

- Flashing Green Lights (13 times) indicate that the lock has been unlatched and will not re-lock when the lights go out.

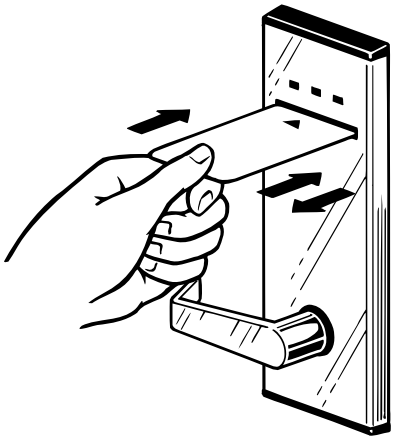
If other lights flash, refer to Section 2.3 for explanations.



2.2.5 Using a Security/Emergency Key in a Lock

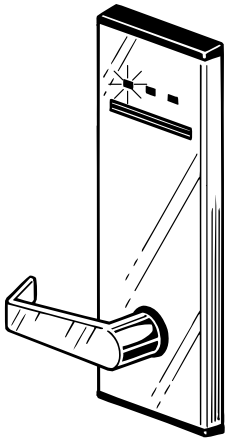
The Security/Emergency is intended to be used for security purposes. It is the only key that will override a dead bolt, privacy switch and electronic lockout to open a door.

Step 1. Insert and remove the keycard in the lock.

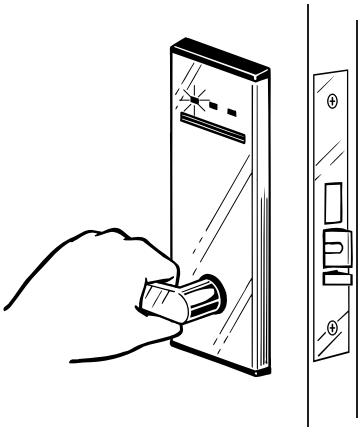


Step 2. The Security/Emergency key will always produce flashing green lights (12 times) and allow the door to be opened. You will get the normal green lights even if the door is dead bolted, the privacy switch is activated or the door is electronically locked.

If other lights flash, refer to Section 2.3 for explanations.



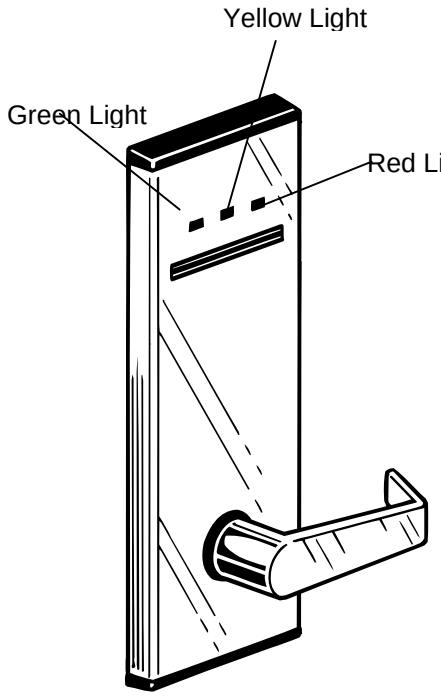
If you turn the handle, you will disengage the dead bolt or the privacy switch. While the Security/Emergency key will override an electronically locked door, it will not permanently remove the lockout (refer to Electronic Lockout keys).



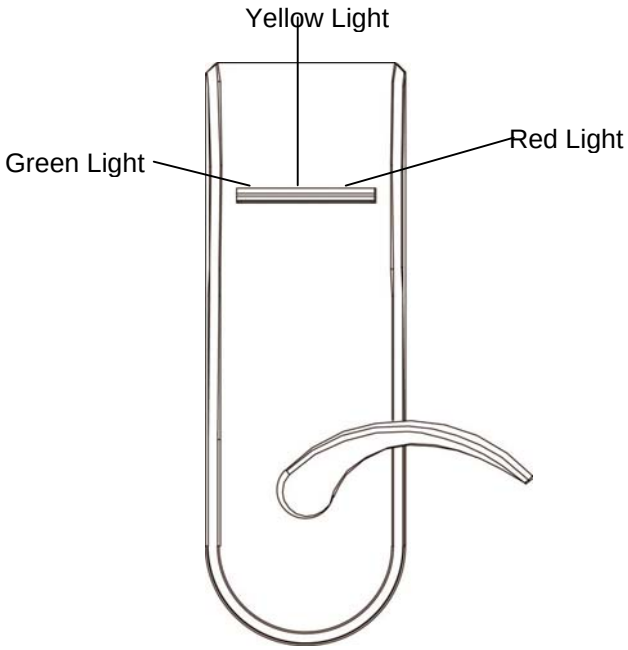
2.3 THE MEANING OF LOCK LIGHTS WHEN USING A KEYCARD

This section explains the different lock lights you can get when you use a standard keycard (guest or master keycard). If you are using a special keycard, refer to Section 7. When you use a keycard, you will normally get a flashing green light for six seconds indicating you can turn the handle and open the door. If you do not get a flashing green light, the lock will display one of the other light patterns listed below.

The MT lock has three light indicators (green, yellow and red) located on the face of the lock. The Adese lock has three light indicators (green, yellow and red) that will illuminate from the opening of reader of the lock. These will flash in various light patterns when a key is used.



MT Lock



Adese Lock

2.3.1 Green Flashing Light

1. Flashing Green Light (12 Times)
This light pattern indicates that the keycard used was a valid current key and is allowed to open the door.

Note: One Yellow flash can occur before the flashing green lights to indicate the key will expire soon. This will begin happening 7 days before the key will actually expire.
One Red flash before the flashing green lights can occur with a Latch/Unlatch key. Refer to Section 2.2.4.

2. Four Fast Green Flashes
This light pattern indicates that the lock reset and has had a problem. Use the keycard again and troubleshoot the lights you get.

2.3.2 Yellow Flashing Light

A yellow flashing light indicates the keycard is not valid or is unable to open the door. There are three different patterns of flashing yellow lights which indicate different things.

1. Flashing Yellow Light (12 Times)
This light pattern indicates that the keycard used was a valid current key but it is not allowed to open the door. This will occur if the door is dead bolted or the privacy switch is activated.

Note: One Red flash before the flashing yellow lights can occur with an Inhibit key (refer to Section 2.2.2) or an Electronic Lockout key (refer to Section 2.2.3).
One Green flash before the flashing yellow lights can occur with an Electronic Lockout key (refer to Section 2.2.3).

2. Fast Flashing Yellow Light (8 Times)
This light pattern indicates that the keycard used was a valid current key but it is not allowed to open the door. This will occur for one of the following reasons:
- the door has been electronically locked out
- the keycard has been inhibited (this can occur for Guest keys if the Inhibit key was used or if a new guest key has been used)
- the keycard has expired.
- a mater key is being used out of shift.

3. Two Yellow Flashes
This light pattern indicates that the keycard used was NOT a valid current key and it is not allowed to open the door. Typical reasons for this include:
- the keycard was canceled out by a new key
- the keycard does not belong to the lock (wrong key, wrong property, etc.)

4. One Yellow Flash
This light pattern indicates that the keycard is a real property key and the lock is Factory programmed or the keycard is an Installation/New Construction key and the lock is a programmed to a real room.

2.3.3 Red Flashing Light

A red flashing light typically indicates the lock's batteries are low or its clock needs updating. The red light will normally flash along with the green or yellow lights.

1. Red Light Flashing ALTERNATELY with Green or Yellow Light (12 Times)
This light pattern indicates that the lock's batteries are low. Once the batteries are changed, the red light will no longer flash.

2. Red Light Flashing SIMULTANEOUSLY with Green or Yellow Light (12 Times)
This light pattern indicates that the lock's clock needs updating. Once the clock is updated (see Section 8.3), the red light will no longer flash.

3. Flashing Red Light (12 Times)
This light pattern indicates that the keycard is a Floor or Section key with the low battery and clock reset hassle feature. For these keys a low battery or clock reset condition will cause the key to give only a flashing red light the first time it is used. If the key is used again, it will get the red light flashing with the green or yellow lights.

4. One or Two Red Flashes
This light pattern indicates that the keycard was used improperly (upside down, backwards or not removed) or the keycard was not encoded (blank key). The red light will not flash immediately - it flashes 6 seconds after the key was inserted.

5. One Long (1 second) Red Light
This light pattern indicates that the keycard was a key that would normally open the door, however, the lock has a motor and was improperly programmed for a solenoid or ECU/RCU hardware mode. The correct lock type must be used to match the Hardware Type. When the lock is reprogrammed with correct the hardware type, it will work normally.

2.3.4 No Lights or Other Lights

If you do not get the normal lights when you use a keycard, it usually indicates some type of problem. Your Lock Installation & Troubleshooting Manual contains detailed troubleshooting procedures for all the light patterns.

1. Two Yellow & Red Light Flashes
This light pattern indicates that the lock could not read the key. This typically indicates that the keycard is worn out or damaged and needs to be replaced.

2. No Lights
No lights will only occur when using a key in the following conditions:
- the Invalid Key Shutdown feature is in effect (wait 2 mins or use a Master key).
- the lock batteries are dead

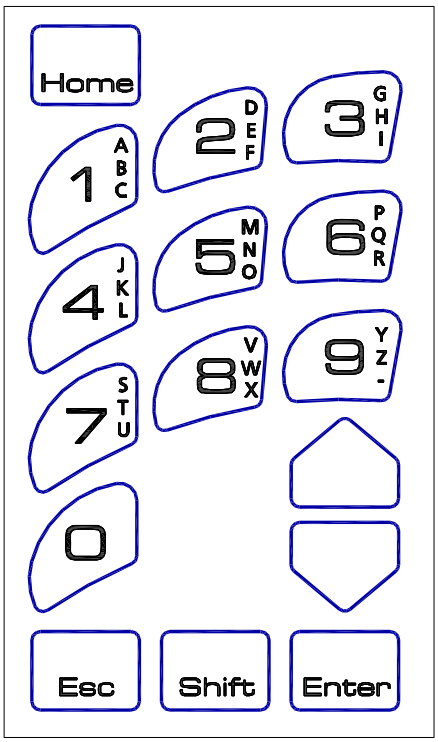
3. All Three Lights Flashing Together
There are several light patterns that will flash all three lights together. These lights usually indicate a problem. Section 14.5.1 explains these lights. You should refer to Section 7.5 to use Special keys to Enter a Problem Lock. You can then troubleshoot the lock problem.

SECTION 3 - SIGNING ON AND ENCODING KEYS

3.1 ENTERING INFORMATION ON THE TERMINAL KEYPAD

The Keypad

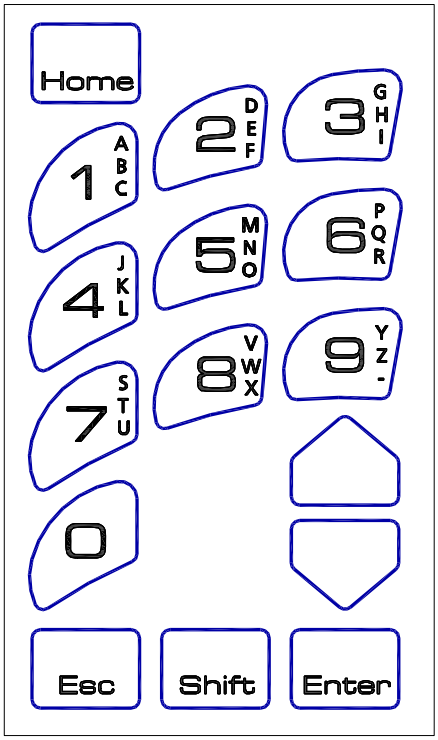
The Hand-Held Terminal keypad is shown below. The keypad will allow you to enter both digits and alphabetic characters. Alphabetic characters are allowed for passwords and room numbers. Whenever you press a key (except the SHIFT key), the terminal will beep to indicate it registered it.



The **0 - 9 keys** are used to enter numbers for input fields. If the cursor is on a menu field or screen, you can also enter the number of the menu item instead of using the ARROW keys to position the cursor on the menu item.

The **A - Z and dash keys** (SHIFT + 1-9 keys) are used to enter letters for input fields. If the cursor is on a menu field or screen, you can also enter the letter of the menu item instead of using the ARROW keys to position the cursor on the menu item.

Each digit key (1-9) has three letters above it. To select the 1st (left) letter, hold down the SHIFT key and press the digit key once. Then release the SHIFT key. For the 2nd (middle) letter, you would press the digit key twice while you hold down the SHIFT key and for the 3rd (right) letter, you would press the digit key three times while you hold down the SHIFT key.



The **ARROW keys** are used to move the cursor from one input field to another. If the cursor is on a menu field, it will move the cursor up or down through the menu items.

The **HOME key** is used to re-enter an input field such as a room number or to move to the previous input field if you are in a menu. This button can be used if you make a mistake while entering the information. The cursor will move to the beginning of the field and allow you to re-enter the info. When you begin entering the new info, the old info will disappear.

The **BACKSPACE key** (SHIFT + ARROW UP key) is used to backspace 1 character. If you make a mistake while entering some information, hold down the SHIFT key and press the ARROW UP. Then release both keys. The cursor will move left 1 character and allow you to re-enter the characters.

The **ESC key** is used for a variety of purposes. It is used when you are done making keys or done with another function and you wish to return to the Password/Sign On screen. It is also used to abort a function before it is completed. For certain transaction functions, you may be returned to a previous menu screen to allow you to select another menu item. If a user is ever in doubt about whether to continue anything, they can press ESC until they are at a point that they can start over.

The **ENTER key** is used to end the input of a field such as a room number and go to the next input field. If a menu item is displayed, it selects the menu item the cursor is on and goes to the next input field. If there are no more input fields, the terminal will go on to the next screen.

3.2 ENTERING INPUT INFO AND MENU SELECTIONS

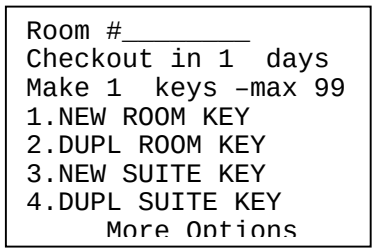
There are a variety of ways the Hand-Held Terminal will use to get input when the user needs to enter something from the keypad. For the most part, it will be obvious what the user needs to enter. There are, however, some short cuts users can use to make their input even faster.

Entering Input Field Information

Input fields require the user to type in the information needed. After entering the number or letter characters, the user would press ENTER. When possible, the terminal will pre-set the information to a standard default value to minimize the input required from the user. If the user likes the default, they simply press ENTER. The Password, Room # and # of days until Checkout fields in the Sign On screens are typical input fields.

Selecting Menu Field Items

When possible, the terminal uses menus for input so the user can easily decide what they want to do. In some cases, the entire menu can not be displayed on the screen. The user can use the ARROW keys to scroll through the menu until they see the selection they want. Each menu item has a number or letter in front of it. If the user is familiar with the menu, they can simply press the NUMBER or LETTER key and the cursor will immediately go to and display that selection. Once the cursor is on the desired selection, the user would press ENTER. A typical menu field is the transaction function field in the Sign On screen.



Input field
Input field
Input field with default
Menu field (see menu below)

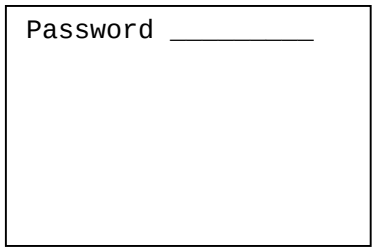
Transaction Function Menu Selections

1.NEW ROOM KEY
2.DUPL ROOM KEY
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
7.PROGRAM LOCKS
8.INTERROGATE LOCKS
9.MISCELLANEOUS
0.IDENTIFY A KEY

3.3 THE PASSWORD AND SIGN ON SCREENS

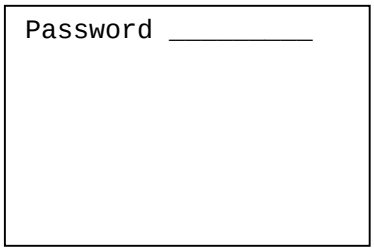
The Password Screen

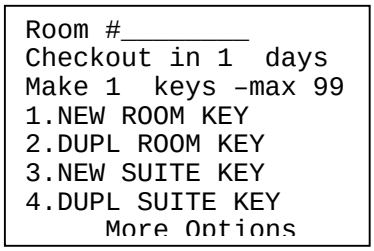
If your property has decided to allow users to sign onto the Hand-Held Terminal and remain signed on for a period of time, the Password Screen will not be displayed for every key or function you wish to make. The time you would remain signed on varies depending on what your property chose (from 1 minute to 8 1/2 hours). If the password screen is displayed, you would enter your 3 to 10 character password and press ENTER.



The Sign On Screens

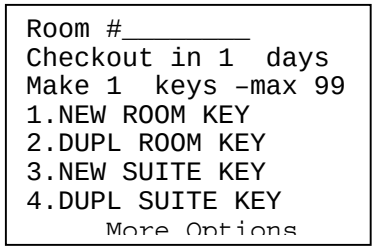
You will typically see one of two Sign On screens when you are ready to make a key or select a function. The screen on the left will appear if your property wants you to enter your password for every key or function you want to select. The screen on the right will appear if you are allowed to sign onto the Hand-Held Terminal for a period of time (see Password Screen above). To "sign off" from the Hand-Held Terminal, you would press ESC at the Sign On screen. The terminal will then return to the Password Screen.





3.4 THE DESKLINC TERMINAL FUNCTION MENUS

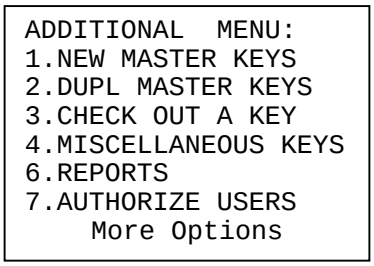
The DeskLinc terminal has several transaction function menus. The sections in this manual will instruct you on what to enter from each menu to do the function you desire. The first menu is accessed from the Sign On screen. The most common functions performed are selected from the Sign On screen menu.



Sign On Screen Transaction Function Menu Selections

1.NEW ROOM KEY
2.DUPL ROOM KEY
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
7.PROGRAM LOCKS
8.INTERROGATE LOCKS
9.MISCELLANEOUS
0.IDENTIFY A KEY

The DeskLinc Computer Terminal has an additional transaction function menu which is displayed when you press 6.ADDITIONAL MENU from the Sign On screen and press ENTER. The menu below would then be displayed. These functions are less frequently performed.



Additional Function Menu Selections

1.NEW MASTER KEYS
2.DUPL MASTER KEYS
3.CHECK OUT A KEY
4.MISCELLANEOUS KEYS
6.REPORTS
7.AUTHORIZE USERS
8.SYSTEM DATE & DST
9.SYSTEM DESIGN

There are also several other menus which will appear such as the MISCELLANEOUS menu accessed by selecting 9 from the Sign On menu, the MASTER KEY LEVEL menu, MISCELLANEOUS KEY menu, REPORTS menu, SYSTEM DATE & DST menu and SYSTEM DESIGN menu accessed by selecting 1, 2, 4, 6, 8 and 9 from the Additional menu).

MASTER KEY LEVEL MENU

```
MASTER KEY LEVEL:
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEY
6.ELECT LOCKOUT KEYS
    MORE OPTIONS
```

Master Key Level Menu Selections

1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEYS
6.ELECT LOCKOUT KEYS
7.INHIBIT KEYS
8.LATCH/UNLATCH KEYS

MISCELLANEOUS KEYS MENU

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

REPORTS MENU

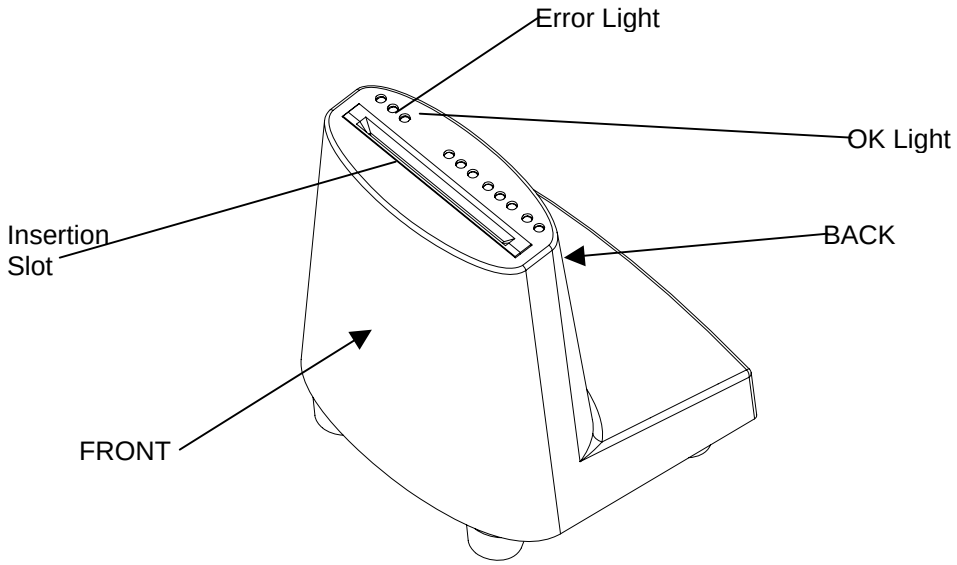
```
REPORTS MENU:
1.TX HISTORY
2.KEY DESIGN
3.USERS & AUTH
```

3.5 ENCODING KEYS

The Keycard Encoder is an insertion device which keycard are inserted and removed from the insertion slot. When the encoder is ready for a keycard to be inserted, the Hand-Held Terminal will display the following message:

```
To Encode Key ID xxx

** INSERT KEY **
 or ESC to stop
```

When the Encoder is ready to receive a key, a solid green light around the insertion slot of the Encoder will illuminate. You have 15-20 seconds to insert a key before the encoder times out.



Encoding Magnetic Strip Keycards:
Insert and remove the keycard with the arrow pointing down and the magnetic strip facing the front of the encoder.

If properly encoded the green OK light will flash and the green lights around the keycard insertion slot will remain lit indicating readiness to encoder another key.

Encoding Memory Keycards:
Insert and hold the keycard with arrow pointing down and the chip facing the back of the encoder. When the green lights flash around the keycard insertion slot, remove the key.

If properly encoded the green OK light will flash and the green lights around the keycard insertion slot will remain lit indicating readiness to encode another key.

If the key was not properly encoded or inserted improperly, the red ERROR light will illuminate, red lights will flash around the keycard insertion slot, the Hand-Held will Beep and display the following error message:

```
K194: KEY REJECTED
Key may be damaged.
Try another key.
** ANY KEY or ESC **
```

Do NOT give the rejected key to the guest. To try making a key again, press ANY KEY to get the IINSERT KEY screen. Then re-insert and remove the keycard.

If you do not insert a key within 15 -20 seconds, the Hand-Held Terminal will display the following:

```
K190:  TIMED OUT
Key Was not inserted

**ANY KEY or ESC**
```

To try making a key again, press ANY KEY to get the INSERT KEY screen. Then re-insert and remove the keycard.

When finished making keys, press ESC to return to the Password or Sign On screen.

3.6 CLEANING THE ENCODER

Your encoders should be cleaned once a week or any time they begin rejecting a lot of keycards. You should use the special cleaning keycard provided by Saflok to clean the encoders. ONLY USE CLEANING KEYCARDS PROVIDED BY SAFLOK. If you use other cleaning keycards, you may damage the encoder parts. You can also use a can of compressed air or air compressor to blow the dust out of the encoding slot.

1. Open the pouch and remove the cleaning keycard.

2. Insert and remove the cleaning keycard like you are making a key, repeat several times.

3. If the cleaning key is very dirty, repeat step 2.

4. If available, spray compressed air down the encoding shaft to blow dust out of the encoding slot.

SECTION 4 - GUEST KEYS

4.1 INFORMATION ON GUEST KEYS

Guest level keys include Room, Suite and Failsafe keys. Room and Suite keys are made during normal system operation. Failsafe keys are pre-made room keys and are only issued if you are unable to make keys at your computer system for some reason. Failsafe keys are covered in detail in Section 6.

A room key typically is designed to operate in only one lock. A Suite key is typically designed to operate several locks for rooms with a connecting door. The lock will only allow one guest key to work in a lock at any time. For instance, if a New Suite key is used, it will not only cancel any previous Suite keys, but it will also inhibit any previously used Room or Failsafe keys.

Guest keys typically do not override a dead bolt, a privacy switch or a lock that is electronically locked out. It is, however, possible to set up your Key Design to allow guest keys to override a dead bolt or privacy switch. In any event, a lock will not accept a New guest key when the dead bolt or privacy switch is activated. This will keep a New guest's key from inadvertently canceling out a current occupant's key if the room was double booked.

Guest keys will continue to work normally even when the lock has low batteries or needs its clock reset. These conditions will, however, result in a red light flashing with the normal lights.

4.1.1 Room #s and Suite Key #s

When your property's Key Design was done, Key #s were assigned to each of the Room and Suite keys in your design. The Room numbers are the same as your lock room numbers. The Suite Key #s may or may not be the same as some of your room numbers. For instance, you may have a Suite Key # 101 key that will work in locks 101 and 103. To determine the Room and Suite Key #s for your property, refer to your Key Design. The Room and Suite Key #s are important to know for the following reasons:
- When you make Room keys, you must enter the Room # at the Sign On screen.
- When you make Suite keys, you must enter the Key # instead of a room #.
- When you interrogate a lock, the Key # will be printed.

4.1.2 Issuing Keys to Guests - When to Make New and Duplicate Keys

Generally, you should make NEW keys for guests that will cancel out any previously issued guest keys. The rule of thumb is: If in doubt, replace all the guests' keys with new keys. The locks will always accept the newest guest key made. Follow the procedures in Section 4.2 to make the keys.

Make NEW guest keys and replace all existing guest keys for:
- New guests that are not joining an existing guest.
- Guest keys that are lost or stolen.
- Guest keys that no longer work.

Make DUPLICATE guest keys for:
- Guests that are joining an existing guest.

You should ALWAYS verify that the guest is registered for the room before making any keys for them. If you have Guest Key Brochures with quick instructions for using the keys, you can write the room # on the brochure and insert the keys in it.

4.1.3 Issuing Failsafe Keys when You Can't Make Keys

If you are unable to make keys for new guests for any reason (such as power or equipment failure), you should get out your Failsafe keys and issue them instead. They will work just like new guest room keys.

Step 1. Look in the Sequence 1 Binder or box for the room #. If it contains keys for the room, issue BOTH of them to the guest.

Step 2. If there are no keys for the room in the Sequence 1 Binder or box, look in the Sequence 2 binder or box. If it contains keys for the room, issue BOTH of them to the guest.

Step 3. If there are no keys for the room in the Sequence 2 Binder or box, look in the Sequence 3 binder or box. If it contains keys for the room, issue BOTH of them to the guest.

Step 4. If there are no keys for the room in any Binder or box, you will not be able to issue keys for the room. You must choose another room or let the guest in their room with a Master key.

ALWAYS ISSUE GUESTS FAILSAFE KEYS FROM THE LOWEST SEQUENCE # BINDER OR BOX. If you issue keys from a higher sequence binder or box, you will automatically cancel out the keys in the lower sequence binders or boxes and cannot issue them to guests. BE SURE TO LET MANAGEMENT KNOW IF YOU HAVE ISSUED FAILSAFE KEYS. They can then be sure to replace them once the system can again make keys.

IF A FAILSAFE KEY ISSUED TO A GUEST DOES NOT WORK:

If issued keys do not work, have some one accompany the guest to the room with a Master key and the Failsafe keys.

- If the guest went to the wrong room, the problem is solved.
- If the Master key did not work either or the door was dead bolted, you will need to return the Failsafe keys in the binder/box and re-room the guest.
- If the Master key worked and the Failsafe keys still did not, you will need to try the next Sequence of Failsafe keys for the room. If you have many Failsafe keys that do not work, it indicates that the Failsafe keys were improperly stored or that previously used Failsafe keys were returned to the binders/boxes. You should notify management of this so they can completely remake all new sets of keys when the computer system is again operational.

4.1.4 Guests Returning Keys

When guests return keys, you can collect them and later re-use them. If you are currently issuing Failsafe keys, follow the procedure below instead. If returned keys are marked up or the mag strip appears to be damaged, you should discard them. A key can be re-encoded several times. If it is no longer usable, the encoder will reject it when you try to make a key.

Failsafe Keys

If you are issuing Failsafe keys to your guests, you must be careful not to return used Failsafe keys back into the binder or box. This is because once they are used, they will be canceled by the next new guest key that is used in the lock. This means that the next time you try to issue a guest the Failsafe keys, they will not work. If you have no keys left for the room in any of your Sequence binders or boxes, you can re-store the keys you get back from the guest in a Sequence binder or box. YOU MUST MARK THE KEYS AND/OR THE ENVELOPE SO YOU WILL KNOW THAT YOU MUST REPLACE THEM WHEN YOUR COMPUTER EQUIPMENT CAN AGAIN MAKE KEYS.

Step 1. Look in all the Sequence Binders or boxes for the room #. If any of them have keys, do not re-sore the keys you get back.

Step 2. If there are no keys for the room in any Sequence Binder or box, mark the keys and/or envelope and re-store them in the Sequence 1 binder or box. YOU MUST REMEMBER TO MARK THEM AS USED KEYS.

4.1.5 Handling Guest Keys that do Not Work

There are a variety or normal situations which can explain why a guest key did not work. Some of these situations may include:
- the key was not used correctly
- the key was made for the wrong room
- the room was double booked and a new guest key canceled or inhibited the original guest's key
- the door is dead bolted or the privacy switch activated
- the key expired do to an extended stay

These situations can be handled quickly by following this procedure. If there is another problem, more extensive troubleshooting procedures can be followed. If you have been issuing Failsafe keys, follow the procedures in Section 4.1.3 instead.

Step 1. First replace all the guests' keys with New keys that will cancel out any previously issued guest keys. Use the keys you originally gave the guest when encoding the new keys. If the encoder rejects them, discard them and use other keys instead.

Step 2. Have someone accompany the guest to the room with a Master key and the new Guest keys.

- If the guest went to the wrong room, the problem is solved.

- If the room is occupied (door is dead bolted or privacy switch activated), you will need to re-room the guest. Use the keys you originally gave the guest when encoding the new keys.

- If the Master key did not work and the door was NOT dead bolted, you will need to re-room the guest and have the lock serviced. Use the keys you originally gave the guest when encoding the new keys. Refer to Section 7.7 to use a PPK and Master key to open a lock

- If the Master key worked and the Guest keys still did not, you will want to re-room the guest and have the lock serviced. Use the keys you originally gave the guest when encoding the new keys. Refer to Section 14.5 to trouble shoot the keycard problem.

4.1.6 Checking Guest Keys Out for Early Departures

If a guest checks out earlier than they originally intended, you may wish to also check them out of the DeskLinc System. This will keep the terminal's from generating an error message (Error 205 or 225) that the room may be occupied the next time some one tries to make a New key. Users without 2.Addl FD authorization will not be able to override this error and make a key.

Step 1. Follow the instructions in Section 4.3 to check the key out of the system.

4.2 MAKING NEW AND DUPLICATE GUEST KEYS

New & Duplicate Guest Keys

A NEW guest key will cancel out all previous guest keys when it is used in a lock. NEW keys should be issued to new guests, guests who have lost their original key or had it mistakenly canceled, etc. When in doubt, replace all the guest's keys with New keys.
A DUPLICATE key will not cancel out the existing guest key and should ONLY be issued to guests joining an already roomed guest.

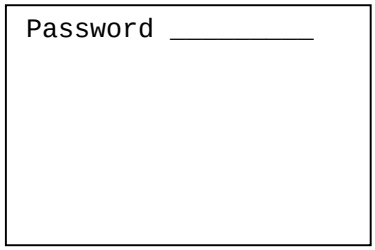
Room, Suite and Connector Keys

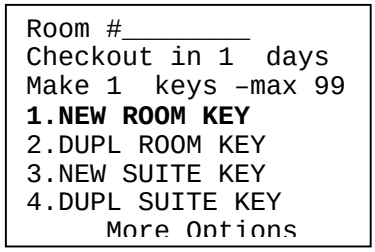
Room keys only operate one room lock. If several rooms connect, your property may also have Suite keys that will operate several room locks. You will need to enter the key # assigned to the specific Suite key instead of the room #. Refer to your Key Design for the correct key #s and the locks they operate.

Making keys from the Sign On Screen

At the Sign On screen:

Step 1. Enter your 3-10 character password (if needed) and press ENTER.





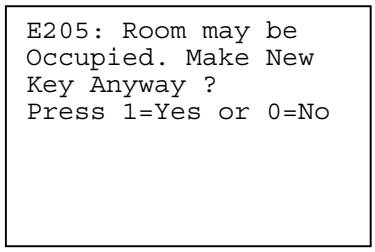
Step 2. Enter the Room # and press ENTER. (For Suite and Connector keys, enter the Key #.)

Step 3. Enter the # of days until checkout and press ENTER. Enter 0 for a guest checking out within a few hours. If the # of days displayed is acceptable, just press ENTER.

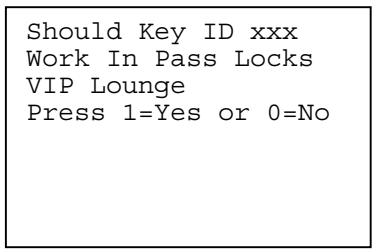
Step 4. Enter the # of keys to be made and press ENTER.

Step 5. For a NEW ROOM KEY: just press ENTER.
For a DUPLICATE ROOM KEY: press 2 and ENTER.
For a NEW SUITE KEY: press 3 and ENTER.
For a DUPLICATE SUITE KEY:press 4 and ENTER.

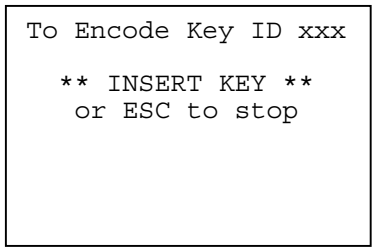
Step 6. If you are making a New key and the previous guest checked out early or you are replacing the current guest's keys with New keys, you may get an error message indicating the room may be occupied before the following screen appears. If you are authorized for 2.Addl FD functions, you will be able to press 1 and continue to make the key. You must be sure to replace all the guest's keys with New keys.



Step 7. If you have selectable pass areas in your design, the following screen will appear. Enter 1 to have the key work in the pass lock shown, or 0 if you do not want the key to work in the pass lock.



Step 8. The following screen should then appear. The xxx in the screen is the Key ID#.



Step 9. Insert and remove a blank or used keycard into the encoder.

Step 10. If you indicated more than one key was to be made, continue making keys. When the number of keys specified has been made the terminal will return to the Password or Sign On screen.

4.3 CHECKING OUT GUEST KEYS

If a guest leaves earlier than originally planned or they change rooms, you can inform the DeskLinc System by checking the key out. If this is not done, the Terminals will display an Error 205 or 225 screen when someone tries to make a new guest key. This error would continue to be displayed until another new key was actually made or until the original guest's checkout date has passed, someone overrides error 205 and makes a new key or until someone checks the key out using this function.

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
     More Options
```

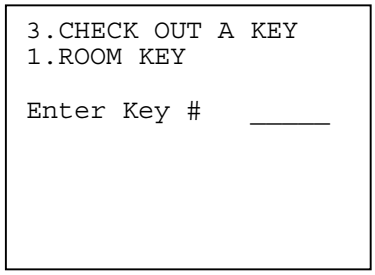
Step 4. The following ADDITIONAL MENU screen will appear. Press 3 or use the ARROW DOWN key to display the 3.CHECK OUT A KEY menu item. Then press ENTER.

```
ADDITIONAL  MENU:
1.NEW MASTER KEYS
2.DUPL MASTER KEYS
3.CHECK OUT A KEY
4.MISCELLANEOUS KEYS
6.REPORTS
7.AUTHORIZE USERS
    More Options
```

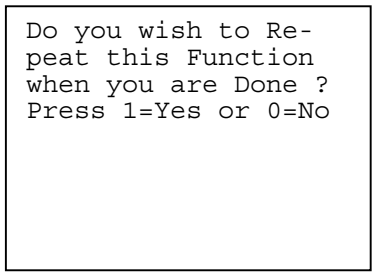
Step 5. The following GUEST KEY LEVEL menu will appear. Use the ARROW DOWN key or press the menu number associated with the guest key you want to select. Then press ENTER.

```
GUEST KEY LEVEL:
1.ROOM KEY
2.SUITE KEY
```

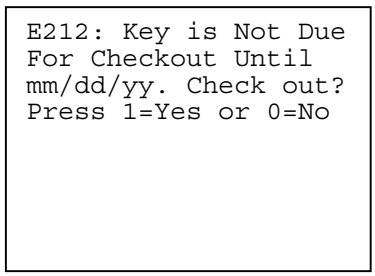
Step 6. The following screen will then appear. The key level you chose in step 5 will display on the second line. In the screen below we chose Room key. Enter the key # you want to check out. For Room keys, this is the Room #. For Suite keys, this should be the Suite Key #. Then press ENTER. (Refer to your Key Design for the Suite key #s.)



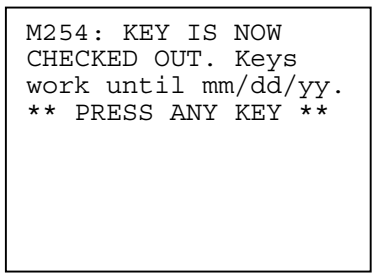
Step 7. If you are authorized for 1.All Auths or 3.Addl FD authorizations, the following screen will now appear. If you are checking out several keys, we suggest you press 1. If you do, you will return to step 4 after you check out a key instead of returning all the way back to the Sign On screen.



Step 8. If the guest is checking out earlier and the key is not considered checked out already, the following screen will then appear. The original check out date is displayed in the screen. To continue to check out the key, simply press 1.



Step 9. The following screen will appear indicating the key is checked out of the system. The screen indicates that the keys will continue to work until the date displayed unless an Inhibit key is used or a New key is made and used. Simply press any key.



Step 10. When you press any key in Step 9 or if you press ESC or time out at any point after step 4, the transaction will end.

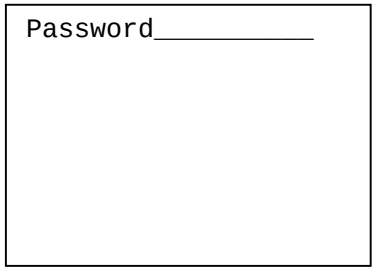
If you indicated 1=Yes in Step 7, you will now return to the ADDITIONAL MENU screen and can go back to step 4 to check out more keys.

If you indicated 0=No in Step 7, you will now return to the Password/Sign On screen and must start over at step 1 to check out more keys.

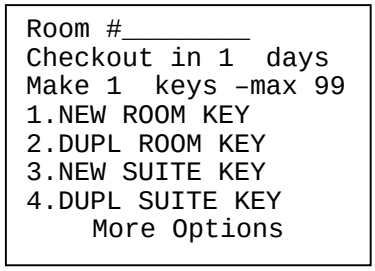
4.4 IDENTIFY A KEY

If a guest reports that their key is not working, you can read the information that was encoded onto the key with the encoder. This function in called Identify a Key which is menu option 0 on the transaction function menu. This function can be used to read any level keycard.

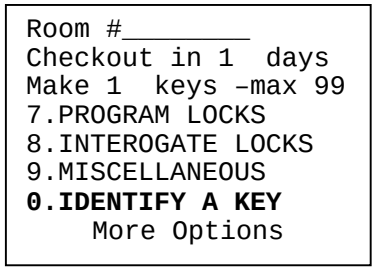
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



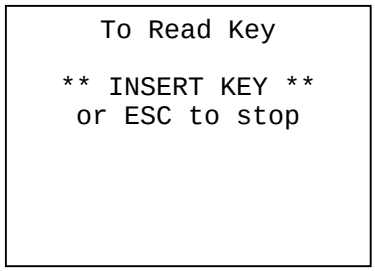
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 0 or use the ARROW DOWN key to display the 0. IDENTIFY A KEY menu item. Press ENTER.



Step 4. The screen instructing you to insert a key will now appear. Insert and remove the keycard.



Step 5. The following screen will appear showing the Key # , level number and ID #. Leave the cursor on 1. Display Key Info and press ENTER.

```
KEY# xxx   MENU:
Level x  ID# xxx
1.Display Key Info
2.Print Key Uses
  ** ESC to End **
```

Note: Menu item 2. Print Keys Uses will only be used if reading a memory keycard (see section 5.5).

Step 6. The Display Key Menu screen will appear. Press the number associated with the menu option to select then press ENTER.

```
DISPLAY KEY MENU:
1. Key Sequence
2. Key Expiration
3. Opening Status
4. shift Hours
5. Pass #s
  ** ESC to End **
```

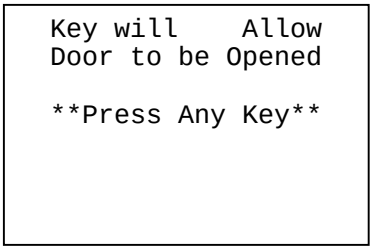
If 1. Key Sequence is selected the following screen will appear showing the date and time the key was made and whether it is the current sequence. Press any key to return to the Display Key Menu.

```
New Key Seq 1st Made
MM-DD-YY  HH:MM A/PM
CURRENT KEY SEQUENCE
  ** Press Any Key**
```

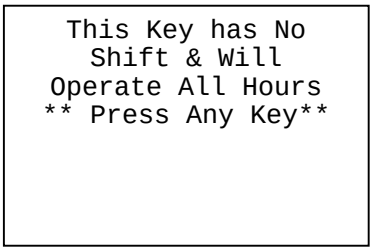
If 2. Key Expiration is selected the following screen will appear showing the date and time the key will expire. Press any key to return to the Display Key Menu.

```
Key Expiration
MM-DD-YY  HH:MM A/PM

  **Press Any Key**
```

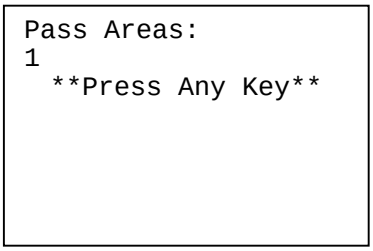
If 3 Opening Status is selected the following screen will appear indicating whether or not the key will allow the door to be opened. Press any key to return to the Display Key Menu.



If 4. Shift Hours is Selected the following screen will appear showing the shift hours assigned to the key.



If 5. Pass #s is selected the following screen will appear indicating an pass area numbers assigned to the key. Press any key to return to the Display Key Menu.

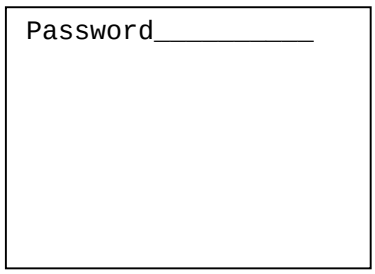


Step 7. Back at the Display Key Menu Press ESC to return the Sign On or Password screen.

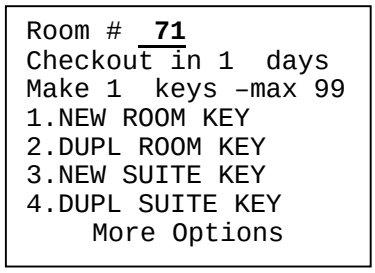
4.5 MAKING LIMITED USE KEYS

A Limited Use key is a standard level key that will open one lock 2 times or until its specified number of days at 11:59p.m., whichever comes first. To have the key expire the same day it is made, select 0 for the # of days to work.

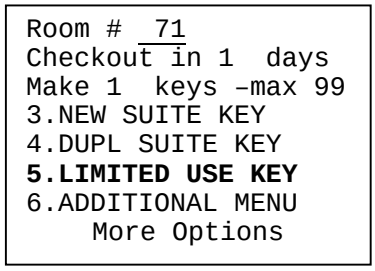
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



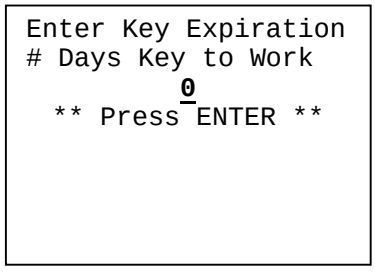
Step 2. Enter the room number. Press ENTER three times to move the cursor to the transaction menu.



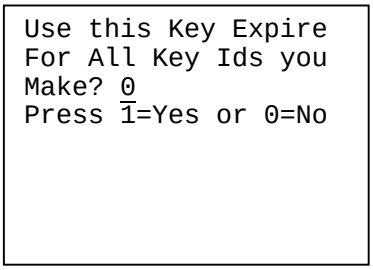
Step 3. Press 5 or use the ARROW DOWN key to display the 5.LIMITED USE KEY. Press ENTER.



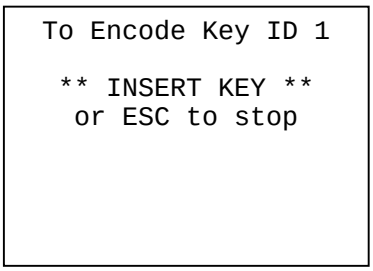
Step 4. Enter the number of days for the key to work. Press ENTER.



Step 5. When the below screen appears, Press ENTER.



Step 6. Insert a key into the encoder.



After the key is inserted and encoded, the terminal will return to the Password screen.

SECTION 5 - MASTER KEYS

5.1 HOW THE VARIOUS MASTER LEVEL KEYS WORK

Master level keys include the following key levels. A master key typically is designed to operate in a group of locks. A lock can be programmed for a master key for each level listed below. Depending on your property's key design, you may have more than one master key for each level to work in a different group of locks and you may have some locks that will not have a master key for one or more of the levels listed. The master level keys work differently and are used for different purposes.

HSKP SECTION KEYS - These keys are typically designed for housekeeping use. There are normally several different Section keys, each operating a different group of locks (normally the group of rooms that one person would clean). Section keys will not override a dead bolt, a privacy switch or a lock that is electronically locked out. These keys also have a low battery & clock reset hassle feature. This requires the key to be used twice in order to enter a room if the lock's batteries are low and need replacing or if the lock's clock time needs updating. This feature is intended to prompt housekeeping to report these lock conditions to the appropriate manager so they will be handled.

HSKP FLOOR KEYS - These keys are typically designed for housekeeping use. There are normally several different Floor keys, each operating a different floor of locks (normally more locks than a Section key covers, such as a group of rooms that an inspector would check after cleaning). Floor keys will not override a dead bolt, a privacy switch or a lock that is electronically locked out. These keys also have a low battery & clock reset hassle feature. This requires the key to be used twice in order to enter a room if the lock's batteries are low and need replacing or if the lock's clock time needs updating. This feature is intended to prompt housekeeping to report these lock conditions to the appropriate manager so they will be handled.

INHIBIT KEYS - These keys are designed for housekeeping inspectors to inhibit (lock out) any working guest keys after a room has been vacated. This ensures that a checked out guest cannot re-enter the room. Inhibit keys will not open a door. When an Inhibit key is used, the current guest Room, Suite or Failsafe key will be locked out so that no guest keys will remain working. The next New guest key will work normally. There is normally only one Inhibit key area, however, more than one is possible.

GRAND MASTER KEYS - These keys are typically designed for employees who will need access to all the rooms. There is normally only one Grand Master key area, however, more than one is possible. These keys will not override a dead bolt, a privacy switch or a lock that is electronically locked out.

SECURITY/EMERGENCY KEYS - These keys are typically designed for employees who will need security or emergency access to all the rooms. There is normally only one Security/Emergency Master key area, however, more than one is possible. These keys will override a dead bolt, a privacy switch or a lock that is electronically locked out.

ELECTRONIC LOCKOUT KEYS - These keys are designed to electronically lock or unlock a room. They will not open a door. When a lock is electronically locked, the only key that will open the door is the Security/Emergency key. When the electronic lockout is removed, all the keys will again operate the lock. There is normally only one Electronic Lockout key area, however, more than one is possible.

LATCH/UNLATCH KEYS - These keys are designed only for entrance doors or meeting room type applications that do not have dead bolts or privacy switches. Guest rooms do not have these keys. When a Latch/Unlatch key is used in a lock, it will leave the lock unlatched or it will re latch a previously unlatched lock. When a lock is unlatched, no keycards are necessary in order to turn the handle and open the door. When the lock is latched, valid keycards must be used to open the door.

5.2 ISSUING AND CONTROLLING MASTER KEYS

5.2.1 Master Key #s, ID#s, Expiration and Shift Times

Key #s: When your property's Key Design was done, Key #s were assigned to each of the master keys in your design. For instance, you may have several Section keys. One could have a Key # 11 and work in rooms 100 through 125. Another could have Key # 12 and work in rooms 126 through 150. Section 10.4 explains how to print your Key Design to determine your Key #s. The Key # is important for the following reasons:
- When you make master keys, you must enter the Key #.
- When you interrogate a lock, the Key # will be printed.
- When you have more than one key for a master level (such as several different Section keys), you will need to write the Key # on the key so employees will know which rooms it works.

ID #s: When you make master keys, the computer system automatically assigns a unique ID # between 1 and 255 to the key. For instance, you may have for copies of a Grand Master #1 key (one for each person who needs one) and they will have ID #s 1, 2, 3 and 4. When you make New keys, the computer begins with ID # 1. The ID # is important for the following reasons:
- When you interrogate a lock, the particular ID # used will be printed. This allows you to determine who went in the room.
- If you need to replace a worn out key, you must enter the ID # when you duplicate the key.
- When you are assigning keys to departments instead of individual employees, you will need to write the ID# on the key so the department can track which ID # an employee signed out.

Expiration: When you make master keys, you can enter the # of days you want the key to work for each ID#. You can choose from 0 to 999 days. If you enter 0, the key will expire (stop working in the locks) at the end of the day you make it. If you choose a number greater than 0, it will expire that many days from the day you make it. When you first make New keys, the computer system will prompt you with a default # of days. When you make Duplicate keys, the computer system will prompt you with the # of days that corresponds to the longest key expiration of the other IDs that you have already made for that master key.

Keycard Expiration Warning: When a master key is getting close to its key expiration date, the lock will provide a warning light when the key is used. A single Yellow light will flash once before the green light flashes. This will begin to occur 7 days before the key actually stops working. You should replace the key before it actually expires.

Shift Times: Masters level keys, except the emergency level, can be programmed to work only during certain shift hours of the day. When the keys is made the user can specify the start and end times of the shift. A key can only have one shift time specified. If the key is used outside the shift time it will not work.

5.2.2 Issuing and Controlling Master Keys

Establishing Master Key Control Sheets
You should establish a control record for master keys which includes the following information. This is important to track in order to be able to identify who used a master key from a lock interrogation report and to know whose keys you must replace when you make New keys.
- Master level (Section, Floor, etc.)
- Key # (refer to Section 10.4 to print your Key Design)
- ID #
- the name of the person or department that was given the key
- sign out & sign in times (if keys are signed out by different people)

When you need to replace a worn out master key, you can verify the key's ID# using the control form. When you make New keys, you can verify all the people who are issued the same level and Key # you are making. You can then be sure to get their old keys back and give them their New key (with the same ID# if desired).
When you interrogate a lock, you can refer to your control sheets to match the level, Key # and ID# with the person it was assigned to.

Labeling Master Keys when You Make Them
In order to be able to identify a master key after you have made it, you will want to mark it with the level (Section, Floor, etc.), key # and ID#. You can use a permanent marker, labels or another suitable marking device.

If you use labels, do not put them on the keys until after you make each key and be sure to apply them to the lower half of the key. This is important to ensure the label cannot get stuck in the lock and will not interfere with encoding the key.

If you use a permanent marker, you can mark the keys before you make them. You should write on the top half of the key so the marking will not wear off. You can write on the bottom half of the key and then cover the writing with clear tape. If you use tape, always write on the bottom half of the key so the tape will not interfere when the key is inserted in the locks.

If you wish to punch a hole in the keycard to use it on a keyring, put the hole on the bottom of the card.

Signing Out Master Keys
If any employees or vendors will sign out master keys, be sure to establish a control sheet and procedures to ensure you will have a record of who had access to the rooms. You may also want the person to sign their name or initials. The keys you use for signing out should be different than the ones permanently assigned to employees. In other words, they should have their own ID# so there is no possibility of confusing who had the key at any time. When a lock is interrogated, you will be able to identify the "sign out" master keys and use the control sheet to determine who had the key at that time.

5.2.3 Initially Making All Your Master Keys

When you first receive your computer system, you will need to make all your master keys.

Step 1. First determine who will need keys and set up your control sheets (see Section 5.2.2).

Step 2 You should now mark or prepare your master key labels (see Section 5.2.2). If you use a permanent marker to label your keys, you should mark each master key you will make. If you use labels, you should make the labels, but do not apply them to the keys. If you are making several keys for any master key, keep in mind that the ID#s will always start at ID# 1.

Step 3 Follow the procedures in Section 5.3 to MAKE NEW MASTER KEYS. You will need to do this function for each of the master level keys. If you use labels on your keys, you should apply the appropriate label after you make each key.

If you are interrupted while making keys and do not make all the ID#s for a particular master key while you are in the NEW MASTER KEYS function, DO NOT use the NEW key function to make the remaining ID#s. You must use the DUPLICATE key function to make the remaining ID#s.

Step 4 Once the new keys are made, you need to distribute them to the appropriate people. It is not necessary to use the new keys in all the locks since there are no old master keys.

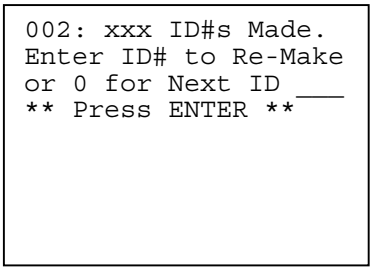
5.2.4 Replacing Damaged or Expired Master Keys

If you need to replace a damaged, worn out or expired master key, you should ALWAYS MAKE A DUPLICATE KEY. If you make a New key, it will cancel out everyone else's other key IDs for that master key # when it is used.

Step 1. You will need to know and enter the ID#s of the keys when you re-make them. If you do not have the key level, key # and/or ID# written on the keys, refer to your control sheets (see Section 5.2.2).

Step 2 If you are re-making keys that have expired, you can simply re-encode them. If you are replacing worn out keys, you should now mark or prepare your master key labels (see Section 5.2.2). If you use a permanent marker to label your keys, you should mark each master key you will make. If you use labels, you should make the labels, but do not apply them to the keys until after you encode the keys.

Step 3 Follow the procedures in Section 5.4 to MAKE DUPLICATE MASTER KEYS. You will need to do this function for each of the additional master keys you are making. When the following screen appears, you should enter the ID# you are re-making and ENTER.



If you use labels on your keys, you should apply the appropriate label after you make each key.

Step 4 Once the keys are made, you should destroy any original worn out keys so there is no possibility they will still work. You can then distribute the re-made keys to the appropriate people. It is not necessary to use the keys in the locks since they are duplicates of the original keys.

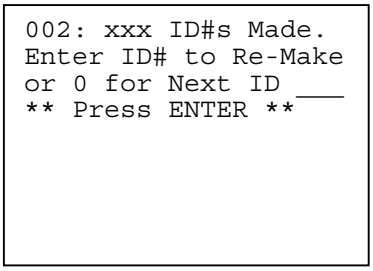
5.2.5 Making Additional Master Keys for Additional Employees

If you need to make additional master keys for new employees, you should ALWAYS MAKE A DUPLICATE KEY. If you make a New key, it will cancel out everyone else's other key IDs for that master key # when it is used.

Step 1. First update your control sheets (see Section 5.2.2) for the new keys. The keys you will make will end up with the next ID#.

Step 2 You should now mark or prepare your master key labels (see Section 5.2.2). If you use a permanent marker to label your keys, you should mark each master key you will make. If you use labels, you should make the labels, but do not apply them to the keys until after you encode the keys.

Step 3 Follow the procedures in Section 5.4 to MAKE DUPLICATE MASTER KEYS. You will need to do this function for each of the additional master keys you are making. When the following screen appears, you should press 0 and ENTER so the computer will generate a new ID#.



If you use labels on your keys, you should apply the appropriate label after you make each key.

Step 4 Once the keys are made, you need to distribute them to the appropriate people. It is not necessary to use the keys in the locks since they are duplicates of the existing keys.

5.2.6 Replacing Lost or Stolen Master Keys

If a master key is lost or stolen, you should immediately replace all the keys for that master level key. You should ALWAYS MAKE NEW KEYS. You should then use one of them in all the locks it is assigned to. This will cancel out the lost or stolen key so it will no longer work.

Step 1. Refer to your control sheets to determine who else will need a new master key (see Section 5.2.2).

Step 2 You should now mark or prepare your master key labels (see Section 5.2.2). If you use a permanent marker to label your keys, you should mark each master key you will make. If you use labels, you should make the labels, but do not apply them to the keys. If you are making several keys for any master key, keep in mind that the ID#s will always start at ID# 1.

Step 3 Follow the procedures in Section 5.3 to MAKE NEW MASTER KEYS. If you use labels on your keys, you should apply the appropriate label after you make each key.

If you are interrupted while making keys and do not make all the ID#s for a particular master key while you are in the NEW MASTER KEYS function, DO NOT use the NEW key function to make the remaining ID#s. You must use the DUPLICATE key function to make the remaining ID#s.

Step 4 Once the new keys are made, immediately have some one take one of the keys and use it in each lock it should work in. The locks should give either flashing green or flashing yellow lights to indicate it accepted the new key. The door does not need to be opened for the lock to accept the new key.

Step 5 You should then distribute the New keys to the appropriate people and retrieve their old keys (they will no longer work).

5.2.7 Periodically Replacing Existing Master Keys with a New Sequence of Keys

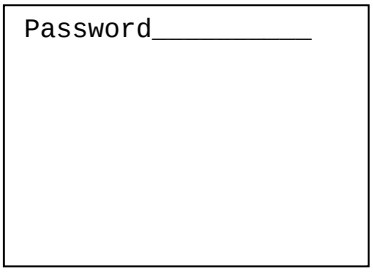
You may periodically want to replace every ones' master keys with new keys. To do this, you can follow the same procedures as 5.2.3. You will, however, need to remember to get their old keys back if you do not just collect them and re-encode them.

Once the new keys are made, immediately have some one take one of the keys and use it in each lock it should work in. The locks should give either flashing green or flashing yellow lights to indicate it accepted the new key. The door does not need to be opened for the lock to accept the new key.

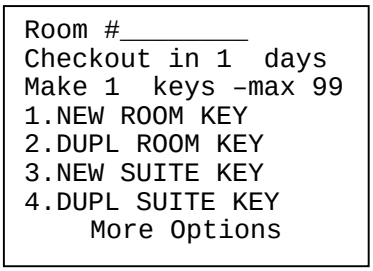
5.3 MAKING NEW MASTER KEYS

New master keys will cancel the previously issued master keys so they will no longer work in the locks. A new master key will ONLY cancel the existing master key of the same level and key #. For instance a New Section #11 key will only cancel previously made Section #11 keys. It will not affect Section #12 keys, Floor #1 keys, etc. ONLY MAKE NEW KEYS IF YOU WILL REPLACE ALL THE CURRENTLY MADE OR ISSUED MASTER KEYS.

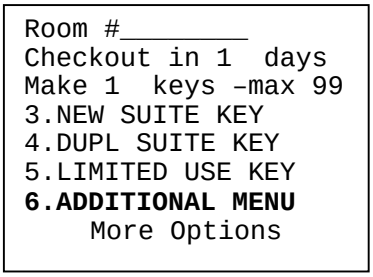
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



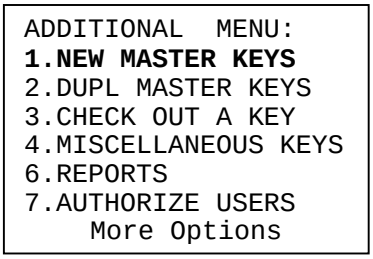
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 1 or use the ARROW UP key to display the 1.NEW MASTER KEYS menu item. Then press ENTER.



Step 5. The following MASTER KEY LEVEL menu will appear. Use the ARROW DOWN key or press the menu number associated with the master key level you want to select. Then press ENTER.

```
MASTER KEY LEVEL:
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEY
6.ELECT LOCKOUT KEYS
    More Options
```

Master Key Level Menu Selections
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEYS
6.ELECT LOCKOUT KEYS
7.INHIBIT KEYS
8.LATCH/UNLATCH KEYS

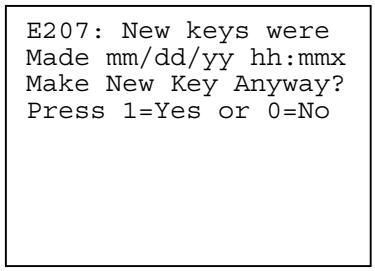
Step 6. A list of master keys for the selected level will display. If all master keys for the level are not display initially, press 0, then ENTER to display more. Otherwise press the number associated to the required key to make then press ENTER.

```
Select Master Key:
1. 1
2. 2
3. 3
4. 4


Enter 1-4 (0=More)__
```

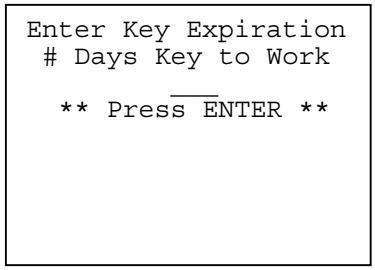
Step 7. If you are authorized for Master keys, the following screen will now appear. If you are making many Master keys, we suggest you press 1. If you do, you will return to step 4 after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

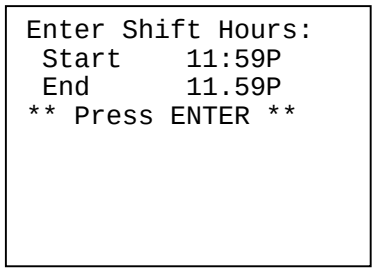
Step 8. The following screen may appear next. If it does, it is intended to remind you that when you make new keys, you will cancel out any existing keys that have already been made (even if you just made some a few minutes ago). If you were unable to make all the ID#s for a key and are trying to make the remaining ones, press 0 and refer to section 5.4 to MAKE DUPLICATE MASTER KEYS. If you know you should be making New keys, press 1 and continue to step 9.



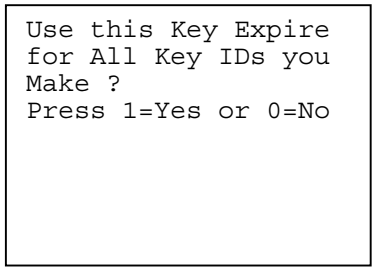
Step 9. The following screen will then appear. Enter the # of days you want the key to work. If you enter 0 days, the key will expire the day it is made. You will notice that a default value is provided. This is a recommended # of days. You can, however, change it to anything from 0 to 999 days by simply entering the new value. Then press ENTER.



Step 10. The following screen will then appear. If necessary, change the shift time settings to the times of the day in which the key should function. Accepting the default start and end settings of 11:59P will allow the key to function all hours of the day.



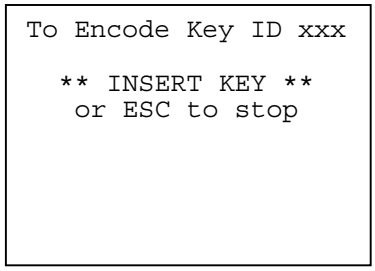
Step 11. The following screen will then appear. If you want all the keys you are going to make to have the same key expiration and shift times that you entered in step 9 and 10, press 1, then ENTER. If you want to enter a different # of days and shift for each Key ID# to work, press 0, then ENTER.



Step 12. The screen instructing you to insert a key should now appear. The Key's ID # is shown on the 1st line (from 1 to 255). Be sure to record this number on the keycard. When you distribute the keys, you will want to assign a person's name to the key ID# you give them. If you interrogate locks later, you will then be able to determine who entered the room by the key ID#.

If you pressed 1 in step 10, this screen will reappear after you make each key ID. Make the number of keys you will want to distribute and then press ESC to end key making.

If you pressed 0 in step 10, you will return to Step 9 after you make the key ID so you can choose a different key expiration and shift time.



Step 13. If you press ESC or time out at any point after step 4, the transaction will end.

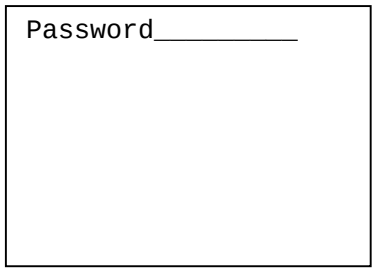
If you indicated 1=Yes in Step 7, you will now return to the ADDITIONAL MENU screen and can go back to step 4 to make more New keys for another Master key. IF YOU WERE UNABLE TO MAKE ALL THE KEYS YOU WANTED FOR A PARTICULAR MASTER KEY AND WISH TO MAKE THE REMAINING KEYS, you should go to Step 4 in Section 5.4 to make Duplicate keys.

If you indicated 0=No in Step 7, you will now return to the Password/Sign On screen and must start over at step 1 to make more New keys for another Master key. IF YOU WERE UNABLE TO MAKE ALL THE KEYS YOU WANTED FOR A PARTICULAR MASTER KEY AND WISH TO MAKE THE REMAINING KEYS, you should go to Step 1 in Section 5.4 to make Duplicate keys.

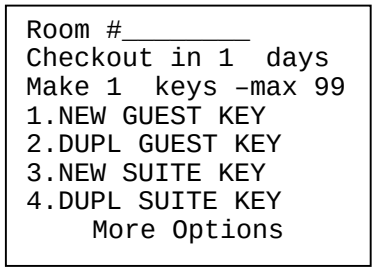
5.4 MAKING DUPLICATE MASTER KEYS

Duplicate master keys will NOT cancel the previously issued or made master keys. You will get the same sequence of key that you got when you last made New master keys for the master level. You will typically make duplicate keys if you are replacing a worn out key, you were unable to make all the key IDs you wanted when you made New keys or you want additional keys for additional people.

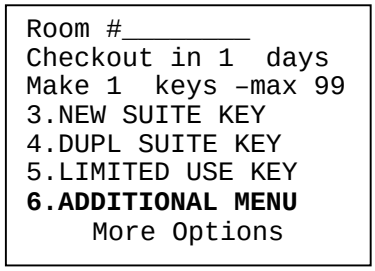
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



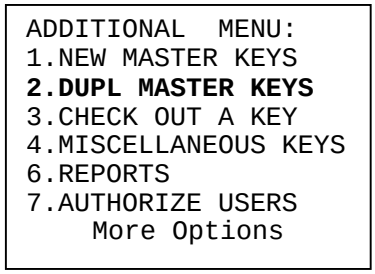
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 2 or use the ARROW DOWN key to display the 2.DUPL MASTER KEYS menu item. Then press ENTER.



Step 5. The following MASTER KEY LEVEL menu will appear. Use the ARROW DOWN key or press the menu number associated with the master key level you want to select. Then press ENTER.

```
MASTER KEY LEVEL:
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEY
6.ELECT LOCKOUT KEYS
    More Options
```

Master Key Level Menu Selections
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEYS
6.ELECT LOCKOUT KEYS
7.INHIBIT KEYS
8.LATCH/UNLATCH KEYS

Step 6. A list of master keys for the selected level will display. If all master keys for the level are not displayed initially, press 0 then ENTER to display more. Otherwise press the number associated with the key to make then press ENTER.

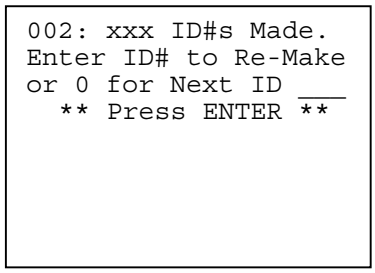
```
Select Master Key:
1. 1
2. 2
3. 3
4. 4


Enter 1-4 (0=More)__
```

Step 7. If you are authorized for Master keys, the following screen will now appear. If you are making many Master keys, we suggest you press 1. If you do, you will return to step 4 after you make keys instead of returning all the way back to the Sign On screen.

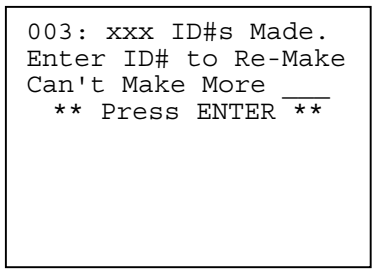
```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 8. One of the following screens will then appear.
If you had previously made less than 255 different key ID#s, you will get screen 002.
If you entered a Key ID# to re-make from Screen 002 and made the key you will get screen 003.
If you had previously made 255 different key IDs, you will also get screen 003. If you don't actually have 255 different keys distributed to people, we recommend that you press ESC to abort this procedure and instead replace all your keys with New keys (Section 5.3).

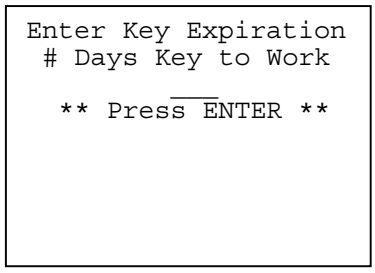
If screen 002 is displayed, the # of key ID#s made so far as indicated on the 1st line. You can make additional keys (with new key ID#s) or you can enter an existing key ID# to replace existing keys. If you want to make more keys to distribute to additional people, enter 0 and press ENTER. If you want to re-make a worn out key, enter the key ID # of the key you want to replace and press ENTER.



If screen 003 is displayed, you are only allowed to re-make existing keys. Enter the key ID # of the worn out key you are re-making and press ENTER.

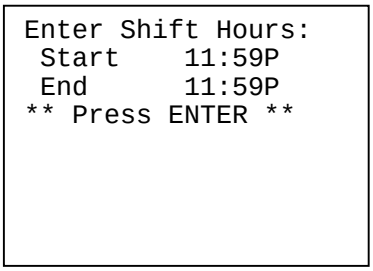


Step 9. The following screen will then appear. Enter the # of days you want the key to work. If you enter 0 days, the key will expire at the end of the day. You will notice that a default value is provided. This is a recommended # of days. You can, however, change it to anything from 0 to 999 days by simply entering the new value. Then press ENTER.

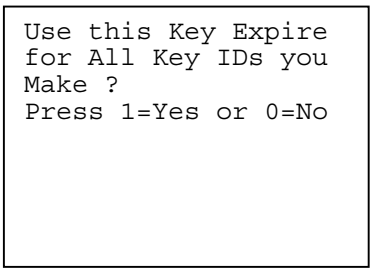


Step 10. The following screen will then appear. If necessary, change the shift time settings to the times of the day in which the key should function. Accepting the default start and end settings of 11:59P will

allow the key to function all hours of the day.



Step 11. The following screen will then appear. If you want all the keys you are going to make to have the same key expiration and shift times that you entered in step 9 and 10, press 1, then ENTER. If you want to enter a different # of days for each Key ID# to work, press 0, then ENTER.

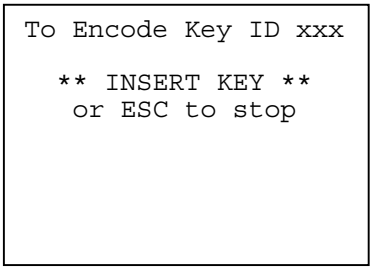


Step 12. The screen instructing you to insert a key should now appear. The Key's ID # is shown on the 1st line (from 1 to 255). Be sure to record this number on the keycard. When you distribute the keys, you will want to assign a person's name to the key ID# you give them. If you interrogate locks later, you will then be able to determine who entered the room by the key ID#.

If you entered a Key ID# to re-make in step 8, you will return to Step 8 after you make the key ID so you can choose a different key ID #.

If you pressed 0 in step 11, you will return to Step 9 after you make the key ID so you can choose a different key expiration and shit time.

Otherwise, this screen will reappear after you make each key ID. Make the number of keys you will want to distribute and then press ESC to end key making.



Step 13. If you press ESC or time out at any point after step 4, the transaction will end.

If you indicated 1=Yes in Step 7, you will now return to the ADDITIONAL MENU screen and can go back to step 4 to make more Duplicate keys for this or another Master key.
If you indicated 0=No in Step 7, you will now return to the Password/Sign On screen and must start over at step 1 to make more Duplicate keys for this or another Master key.

5.5 MEMORY KEYCARD USE REPORT

When a memory keycard is encoded to function as any type of master key, records of the locks in which the key was used in are stored on the key. The key uses and additional key information can be printed at any time to view the key's activity.

Required Equipment
1. Saflok system with memory keycard encoder
2. Saflok memory keys
3. Locks with memory keycard readers
4. Printer

Memory Keycard Information

Memory-chip size (bits)	Record of Uses	Part#
2KB	24	10390
8KB	118	10380
64KB	1014	10370

Process for Reading Memory Keycards:

1. Reading keycard
2. Printing report
3. Reading report

5.5.1 Reading and Printing Memory Keycard Uses

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

```
Password__________
```

Step 2. Press ENTER three times to move the cursor to the transaction menu.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
1.NEW ROOM KEY
2.DUPL ROOM KEY
3.NEW SUITE KEY
4.DUPL SUITE KEY
    More Options
```

Step 3. Press 0 or use the ARROW DOWN key to display the 0. IDENTIFY A KEY menu item. Press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
7.PROGRAM LOCKS
8.INTEROGATE LOCKS
9.MISCELLANEOUS
0.IDENTIFY A KEY
    More Options
```

Step 4. The screen instructing you to insert a key should now appear. Insert the keycard into the encoder and hold it in place.

```
     To Read Key

  ** INSERT KEY **
   or ESC to stop
```

Step 5. While the key is being read the following screen will appear.

```
M084 Please wait

Reading Staff Key
```

Step 6. When the encoder has finished reading the key, the green lights around the insertion slot will flash. Remove the key and the following screen will appear. Press 2 or use the ARROW DOWN key to display the 2. Print Key Uses menu item. Then press ENTER.

```
KEY# 71   MENU:
Level 12  ID# 1
1.Display Key Info
2.Print Key Uses
  ** ESC to End **
```

Note: Menu item 1. Display Key Info will display on screen the information regarding the lock code on the keycard (see Section 4.4).

Step 7. Press 1 to display 1. Key Uses in Locks menu item. Press ENTER.

```
KEY REPORT MENU:
1.Key Uses in Locks
2.Report Explanation
  ** ESC to End **
```

Step 8 . You can now enter the # of days back you want the report to print. The default is 0 which will print all entries on the keycard.

```
S007: For Lock xxxxx
Enter # of days back
to Print 0__ (0=all)
 ** ESC to Abort **
```

Step 9. The following screen will appear. Select 1 if the report should only show records of key uses where the key was allowed to open. Select 0 if the report should show all records of key uses.

```
Do you wish to Only
Print Logs where Key
could open the Door?
Press 1=Yes or 0=No
```

Step 10. Screen M083 will appear. Connect the printer to the terminal. Press ANY KEY.

```
M083:Connect Printer
to the Terminal and
   Press Any Key.
* or ESC to Abort *
```

Step 11. Screen M082 will display while the report is printing

```
M082: PLEASE WAIT
 Sending Report to
Terminal's Printer
*** ESC to Stop ***
```

Step 12. After the report has finished printing. The KEY REPORT MENU screen will appear. Press 2 then ENTER for menu item 2. Report Explanation to print a report that will help with interpreting the key uses report.

```
KEY REPORT MENU:
1.Key Uses in Locks
2.Report Explanation
  ** ESC to End **
```

Sample Key Interrogation Report

PAGE 1 08-17-2006 02:53PM DST PROPERTY NAME TERMINAL #1

KEY INTERROGATION REPORT: TX # 042 REPORT # 1

_REPORT FOR: KEY # 11 LEVEL 9, ID # 1
- Key will Open a Door
- Shift Houre: 11:59PM to 11:59PM
- Key Expires: 08-17-2007 11:59PM
Pass #s: None
New Key Sequence made: 08-17-2006 1:00PM - CURRENT KEY SEQUECE
Key ID was Assigned to: Unavailable
Key Made On: Information Unavailable

Report Date Format Usde: MM-DD-YYYY
Report From: 01-01-1980 to 12-31-2107 11:59PM
Report includes ALL Locks Key was Used in

REC NO.	LOCK#	LET OPEN	DIAG ERROR	LOCK DATE & TIME	TIME SET?	DEAD BLT?	LOW BAT?	LOCK PROB?	LOCK LTCHD?	NEW KEY?
1)	101	Y	0	08-17-2006 01:54PM	Y	N	N	N	Y	N
2)	104	Y	0	08-17-2006 01:17PM	Y	N	N	N	Y	N
3)	107	N	154	08-17-2006 01:15PM	Y	Y	N	N	Y	N

Sample Key Interrogation Explanation Report

PAGE 1 08-17-2006 02:53PM DST PROPERTY NAME TERMINAL #1

KEY INTERROGATION REPORT: TX # 042 REPORT # 1

KEY INTERROGATION REPORT EXPLANATION

STATUS INFORMATION:

LET OPEN? Indicates if the key allowed the door to be opened.
DIAG ERROR: If the key was not allowed to open the door, an error code is logged. Refer to error explanations below.
TIME SET? Indicates if the lock's date & time was set when the key was used. If NO, the lock's clock needs to be reprogrammed.
DEAD BLT?: Indicates if the dead bolt or privacy switch was activated when the key was used.
LOW BAT?: Indicates if the lock's batteries are low & need changing.
LOCK PROB?: Indicates if the motorized lock was not relatching properly & needs service.
LOCK LTCHD?: Indicates if the lock was supposed to be latched (only unlatches when a key is used) vs Unlatched (no keys required to open door).
NEW KEY?: Indicates if the lock stored the key as a new key.

ERROR EXPLANATIONS:

A list of possible diagnostic error codes will appear on the printout. To view the list print the report.

SECTION 6 - FAILSAFE KEYS

6.1 INFORMATION ON FAILSAFE KEYS

6.1.1 Failsafe Sequences and Key Expiration

Failsafe keys should be pre-made and stored for each guest room. If for any reason, you are unable to use your computer system to make new guest keys, you will be able to issue new guests a set of Failsafe keys. Failsafe keys are a VERY important safe-guard for your property since you never want to be in a position where you cannot issue guests keys.

Key #: When making Failsafe keys, you will be asked to enter the Key #. Unless otherwise indicated in your Key Design, the Key # is the same as the room #. Section 10.4 explains how to print Report 3 of your key design information for Failsafe keys if you have any questions.

Failsafe Sequences: Depending on the design your property requested, you will need to store 2 or 3 sequences of Failsafe keys for each room. Each sequence or set corresponds to a New set of keys that will cancel previous keys. This allows you to turn the room over several times. We recommend that you make 2 keys for each sequence in case you have more than one guest for a room. To determine the # of Sequences your system is set up for, you can print Report 1 of your Key Design (Section 10.4) or you can view and change the information by selecting the system default function (Section 15.2.2 - 2.Key Defaults - 2.Failsafe Info).

Failsafe Key Expiration: Failsafe keys work just like guest room keys except they will expire based on when they are used rather than based on a particular check out date. The number of days a Failsafe key will work depends on your property design. A typical setting is 7 days. When a new Sequence of Failsafe keys is used in a lock, the lock will add 7 days to the current date and store it as the date that it will consider that Sequence of Failsafe keys to be expired. To determine the # of expiration days your system is set up for, you can print Report 1 of your Key Design (Section 10.4) or you can view and change the information by selecting the system default function (Section 15.2.2 - 2.Key Defaults - 2.Failsafe Info).

6.1.2 Making Initial Sets of Failsafe Keys

When you first get your DeskLinc computer system, you will need to make all the sequence sets of Failsafe keys for each room. If you found that many of your Failsafe keys did not work when they were issued, you should also follow this procedure to remake all your keys. This procedure will refer to procedures for Making New Failsafe Keys which is detailed in Section 6.2.

Step 1. First check your system design information to determine how many sequences or sets (2 or 3) of Failsafe keys you need to make and store for each room. You will also need to determine and setup how you will store the Failsafe keys. The following methods have been used:

Failsafe Binders - This method entails storing Failsafe keys in loose-leaf binders with plastic pocket sheets. These can be purchased from your Saflok supplier if you desire. You would need a separate binder for each sequence of Failsafe keys - labeled Sequence 1, Sequence 2 and, if applicable, Sequence 3. In each binder, you would have plastic pocket sheets designed to hold sports cards. Each sheet has 9 pockets. You would label each pocket with one of the room #s and include enough sheets in each binder to have a pocket for every guest room.

Failsafe Envelopes in Boxes - This method entails storing Failsafe keys in small coin-sized envelopes and boxes. You would need a separate box for each sequence of Failsafe keys - labeled Sequence 1, Sequence 2 and, if applicable, Sequence 3. You would also need coin-size envelopes to put each set of

Failsafe keys into. For 3 sequences, you will need 3 times the number of rooms in your property and for 2 sequences, you will need 2 times the number of rooms in your property. For each room in your property, label an envelope with the room # and the Sequence #. You would then store all the Sequence 1 keys in the Sequence 1 box, the Sequence 2 keys in the Sequence 2 box, etc.

Step 2. You must now make the Failsafe keys and place them in the appropriate binder pocket or envelope and box. You will first make all the Sequence 1 sets for all the rooms. Follow the procedure in Section 6.2 to make New Failsafe keys. Start with the first room # and when you are asked if you want to repeat the function when you are done, indicate 1 for yes. This will let you make the keys for the next room faster. We recommend that you make 2 keys when you are told to insert a key, then press ESC. If you forget to make 2 keys and only make 1, DO NOT make New keys again to get the 2nd key. Instead, wait until you are done making all the sequences. Then follow the instructions in Step 5. You would then insert the keys in the Sequence 1 binder pocket for the room or in the Sequence 1 envelope for the room. You should repeat this step for each room until you have made all the Sequence 1 keys.

Step 3. You should now make all the Sequence 2 sets for all the rooms. Follow the same procedure as in step 2 except store the keys in the Sequence 2 binder or box.

Step 4. If your design indicates you are keeping 3 Failsafe Sequences, you should now make all the Sequence 3 sets for all the rooms. Follow the same procedure as in step 2 except store the keys in the Sequence 3 binder or box.

Step 5. If you forgot to make 2 keys and only made 1 for any room Sequence, you can now make the missing 2nd key. Follow the instructions in Section 6.3 to make Duplicate Failsafe Keys. You would then store the 2nd key with the 1st key.

Step 6. Now that all the keys are made, you should make sure your Front Office employees are instructed on where the keys will be kept and how to issue them if they are needed. Remember to instruct your evening and graveyard shifts.

6.1.3 Issuing Failsafe Keys to Guests

If you are unable to make keys for new guests for any reason (such as power or equipment failure), you should get out your Failsafe keys and issue them instead. They will work just like new guest room keys.

Step 1. Look in the Sequence 1 Binder or box for the room #. If it contains keys for the room, issue BOTH of them to the guest.

Step 2. If there are no keys for the room in the Sequence 1 Binder or box, look in the Sequence 2 binder or box. If it contains keys for the room, issue BOTH of them to the guest.

Step 3. If there are no keys for the room in the Sequence 2 Binder or box, look in the Sequence 3 binder or box. If it contains keys for the room, issue BOTH of them to the guest.

Step 4. If there are no keys for the room in any Binder or box, you will not be able to issue keys for the room. You must choose another room or let the guest in their room with a Master key.

ALWAYS ISSUE GUESTS FAILSAFE KEYS FROM THE <u>LOWEST</u> SEQUENCE # BINDER OR BOX. If you issue keys from a higher sequence binder or box, you will automatically cancel out the keys in the lower sequence binders or boxes and cannot issue them to guests. BE SURE TO LET MANAGEMENT KNOW IF YOU HAVE ISSUED FAILSAFE KEYS. They can then be sure to replace them once the system can again make keys.

IF A FAILSAFE KEY ISSUED TO A GUEST DOES NOT WORK:

If issued keys do not work, have some one accompany the guest to the room with a Master key and the Failsafe keys.

- If the guest went to the wrong room, the problem is solved.
- If the Master key did not work either or the door was dead bolted, you will need to return the Failsafe keys in the binder/box and re-room the guest.
- If the Master key worked and the Failsafe keys still did not, you will need to try the next Sequence of Failsafe keys for the room. If you have many Failsafe keys that do not work, it indicates that the Failsafe keys were improperly stored or that previously used Failsafe keys were returned to the binders/boxes. You should notify management of this so they can completely remake all new sets of keys when the computer system is again operational.

6.1.4 Guests Returning Failsafe Keys

If you are issuing Failsafe keys to your guests, you must be careful not to return used Failsafe keys back into the binder or box. This is because once they are used, they will be canceled by the next new guest key that is used in the lock. This means that the next time you try to issue a guest the Failsafe keys, they will not work. If you have no keys left for the room in any of your Sequence binders or boxes, you can re-store the keys you get back from the guest in a Sequence binder or box. YOU MUST MARK THE KEYS AND/OR THE ENVELOPE SO YOU WILL KNOW THAT YOU MUST REPLACE THEM WHEN YOUR COMPUTER EQUIPMENT CAN AGAIN MAKE KEYS.

Step 1. Look in all the Sequence Binders or boxes for the room #. If any of them have keys, do not re-sore the keys you get back.

Step 2. If there are no keys for the room in any Sequence Binder or box, mark the keys and/or envelope and re-store them in the Sequence 1 binder or box. YOU MUST REMEMBER TO MARK THEM AS USED KEYS.

6.1.5 Replacing Failsafe Keys that Have Been Issued

If you have issued Failsafe keys to guests, you will want to replace any sequences that were used once you are again able to make keys at your computer system. This will always ensure you have all the sequences or sets of keys for each room should you need to issue them in the future. If you found that many of your Failsafe keys did not work when they were issued, you should make all new sets of keys (refer to Section 6.1.2) instead of following this procedure.

Step 1. First go through all your Failsafe Sequence binders/boxes and remove any keys that are marked as used (refer to Section 6.1.4 Guests Returning Failsafe Keys).

Step 2. To make sure the Failsafe keys were not issued out of order, you can follow this procedure. If someone issued Sequence 2 keys when Sequence 1 keys existed, the Sequence 1 keys will no longer work. Check through your Sequence 3 binder/box. If the keys are missing, check for keys in the Sequence 1 and 2 binders/boxes. If keys exist for the room, remove them - you will need to replace them. Next go through your Sequence 3 binder/box. If the keys are missing, check for keys in the Sequence 1 binder/box. If keys exist for the room, remove them - you will need to replace them.

Step 3. You will now need to "re-sequence" the keys in the binders/boxes. Check through your Sequence 1 binder/box. If the keys are missing, check for keys in the Sequence 2 binder/box. If keys exist move them to the Sequence 1 binder/box. If the keys are also missing from the Sequence 2 binder/box, check your Sequence 3 binder/box. If keys exist move them to the Sequence 1 binder/box.

If you have a Sequence 3 binder/box, now check through your Sequence 2 binder/box. If the keys are missing, check for keys in the Sequence 3 binder/box. If keys exist move them to the Sequence 2

binder/box.

Step 4. You must now replace the missing Failsafe keys in each Sequence binder/box. You will first make missing keys for the Sequence 1 binder/box. Follow the procedure in Section 6.2 to make New Failsafe keys. Start with the first room # and when you are asked if you want to repeat the function when you are done, indicate 1 for yes. This will let you make the keys for the next room faster. We recommend that you make 2 keys when you are told to insert a key, then press ESC. If you forget to make 2 keys and only make 1, DO NOT make New keys again to get the 2nd key. Instead, wait until you are done making all the sequences. Then follow the instructions in Step 7. You would then insert the keys in the Sequence 1 binder pocket for the room or in the Sequence 1 envelope for the room. You should repeat this step for each room until you have made all the missing Sequence 1 keys.

Step 5. You should now check through the Sequence 2 binder/box for missing keys. Follow the same procedure as in step 4 except store the new keys in the Sequence 2 binder or box.

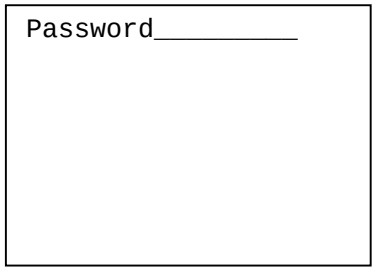
Step 6. If your design indicates you are keeping 3 Failsafe Sequences, you should now check through the Sequence 3 binder/box for missing keys. Follow the same procedure as in step 4 except store the new keys in the Sequence 3 binder or box.

Step 7. If you forgot to make 2 keys and only made 1 for any room Sequence, you can now make the missing 2nd key. Follow the instructions in Section 6.3 to make Duplicate Failsafe Keys. You would then store the 2nd key with the 1st key.

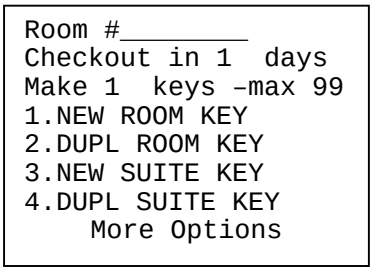
6.2 MAKING NEW FAILSAFE KEYS

When making your initial sets of Failsafe keys or replacing used Failsafe keys, you will always make NEW Failsafe keys. Typically, you will want to make 2 keys for each Sequence set. If you only make 1 key for some reason and want to make a 2nd one, you should wait until you have made all your New Sequence sets and then use the procedure in Section 6.3 to make a Duplicate key for the missing 2nd key.

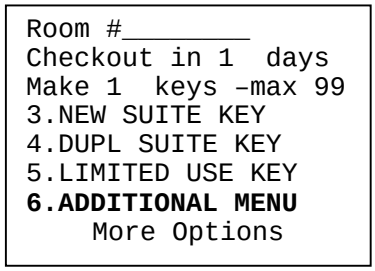
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



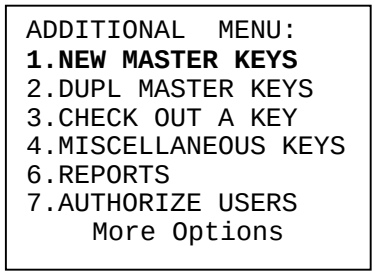
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 1 or use the ARROW UP key to display the 1.NEW MASTER KEYS menu item. Then press ENTER.



Step 5. The following MASTER KEY LEVEL menu will appear. Press 1 or use the ARROW key to select 1.FAILSAFE KEYS. Then press ENTER.

```
MASTER KEY LEVEL:
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEY
6.ELECT LOCKOUT KEYS
    More Options
```

Step 6. A list of failsafe keys will display. Twelve failsafe keys will initially display, press 0 to display more. Otherwise press the number associated to the required failsafe key to make.

```
Select Master Key:
1. 101    7.107
2. 102    8.108
3. 103    9.109
4. 104   10.110
5. 105   11.111
6. 106   12.112
Enter 1-12(0=More)__
```

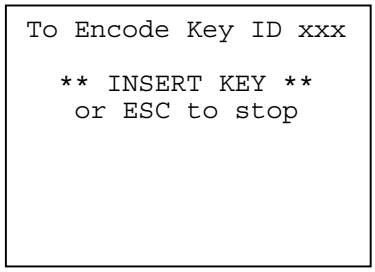
Step 7. The following screen will now appear. If you are making many Failsafe keys, we suggest you press 1. If you do, you will return to step 4 after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
 peat this Function
 when you are Done ?
 Press 1=Yes or 0=No
```

Step 8. The following screen will appear asking you to indicate the number of days you would like the failsafe key to work once it is first used in the lock. Type the number of days and then press ENTER.

```
Enter Key Expiration
#  Days key to Work
   __
  **Press ENTER**
```

Step 9. If you are authorized for Failsafe keys, the screen instructing you to insert a key should now appear. Make a total of two keys and insert them in your Failsafe Sequence binder/box. Then press ESC to end key-making.



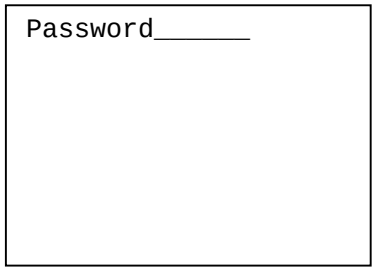
If you indicated 1=Yes in Step 7, you will now return to the ADDITIONAL MENU screen and can go back to step 4 to make more keys.

If you indicated 0=No in Step 7, you will now return to the Password/Sign On screen and must start over at step 1 to make more keys.

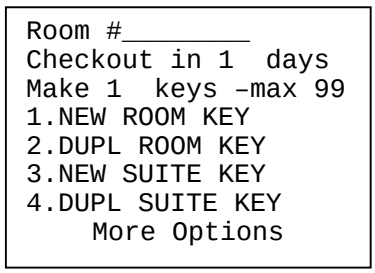
6.3 MAKING DUPLICATE FAILSAFE KEYS

You would ONLY make duplicate Failsafe keys if you did not actually make 2 keys for each sequence when you were making NEW Failsafe keys.

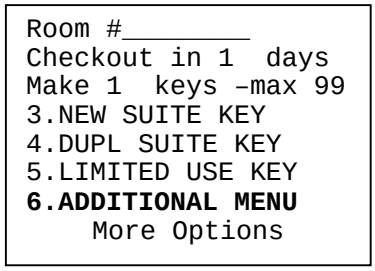
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



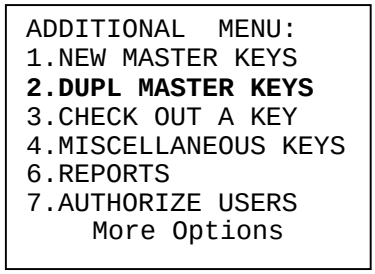
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 2 or use the ARROW DOWN key to display the 2.DUPL MASTER KEYS menu item. Then press ENTER.



Step 5. The following MASTER KEY LEVEL menu will appear. Press 1 or use the ARROW UP key to select 1.FAILSAFE KEYS. Then press ENTER.

```
MASTER KEY LEVEL:
1.FAILSAFE KEYS
2.HSKP SECTION KEYS
3.HSKP FLOOR KEYS
4.GRAND MASTER KEYS
5.SECURITY/EMERG KEY
6.ELECT LOCKOUT KEYS
    More Options
```

Step 6. A list of failsafe keys will display. Twelve failsafe keys will initially display, press 0 then ENTER to display more. Otherwise press the number associated to the required failsafe key to make then press ENTER.

```
Select Master Key:
1. 101    7.107
2. 102    8.108
3. 103    9.109
4. 104   10.110
5. 105   11.111
6. 106   12.112
Enter 1-12(0=More)__
```

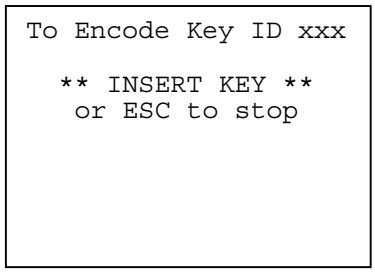
Step 7. The following screen will now appear. If you are making many Failsafe keys, we suggest you press 1. If you do, you will return to step 4 after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 8. If you are authorized for Failsafe keys, the following screen will now appear. The first line will indicate how many sequences you currently should have stored. Enter the Sequence # of the Failsafe key you are duplicating and press ENTER.

```
001: x Failsafe Seqs
are currently Stored
Enter Seq to Make _
  ** Press ENTER **
```

Step 9. The screen instructing you to insert a key should now appear. Make the missing 2nd key and insert it with your 1st key in your Failsafe Sequence binder/box. Then press ESC to end key-making.



If you indicated 1=Yes in Step 7, you will now return to the ADDITIONAL MENU screen and can go back to step 4 to make more keys.

If you indicated 0=No in Step 7, you will now return to the Password/Sign On screen and must start over at step 1 to make more keys.

SECTION 7 - MISC SPECIAL KEYS FOR TROUBLE SHOOTING

7.1 THE VARIOUS SPECIAL KEYS & HOW THEY WORK

Special keys are used for trouble shooting lock problems. They allow you to enter a problem lock and to turn on LED Diagnostics. These keys are designed to work in all the locks in your property but will never open a door.

PRIMARY PROGRAM KEY (PPK)- These keys are used with the E2 Erase key and LED Diagnostics key. They can also be used with a Master key to override invalid lock mode conditions and open a door. The PPK key produces a slow flashing yellow light for 20 seconds when it is used.

SECONDARY PROGRAM KEY (SPK)- These keys are similar to PPK keys and are a backup secondary key in case a PPK key does not work. They can be used with the E2 Erase key and LED Diagnostics key. They can also be used with a Master key to override invalid lock mode conditions and open a door. The SPK key produces a slow flashing yellow light for 20 seconds when it is used.

LED DIAGNOSTICS KEY - This key is used to turn a lock's LED Diagnostics feature on and off. LED Diagnostics is used to determine exactly why a key does not work in a lock. Section 14.5.2 covers this in detail. To turn on LED Diagnostics, the LED Diagnostics key is used after first using the PPK key or SPK key. When the LED Diagnostics key is used, yellow and green lights will flash together 3 times. To turn off LED Diagnostics, the key is used by itself. LED Diagnostics keys do not have ID#s and do not expire in the locks.

E2 ERASE KEY - This key is used to completely erase the lock's memory. When a lock is erased, it goes into Mode 1 and no keycards will work until it is programmed again. Refer to Section 14.5.1 for an explanation of the Mode lights that keys will produce. The E2 Erase key can only be used after first using the PPK key. When the E2 Erase key is used, yellow and green lights will flash together 2 times, then the yellow light will flash once. E2 Erase keys do not have ID#s and do not expire in the locks.

DISPLAY KEYS - These keys are used to display various lock conditions through its LED lights. They do not require any key to be used before them and they do not affect any keys working in the lock. The Lock Installation Manual refers to using these keys when installing a lock to test the hardware. Most often, however, a Display key is used to verify whether a lock is functioning if other keys produce no lights when they are used. Display keys do not have ID#s and do not expire in the locks. Display keycards may include the following:

- Display EPROM Version (Lock's program version)
- Display Clock Time
- Display Clock Date
- Display Knob Turn Switch Status
- Display Dead Bolt/Privacy Switch Status
- Display Low Battery Status

7.2 ISSUING AND CONTROLLING SPECIAL KEYS

7.2.1 PPK & SPK Key #s, ID#s and Expiration

Key #s: When your property's Key Design was done, Key #s were assigned to each of the PPK & SPK master keys in your design. Section 10.4 explains how to print your Key Design to determine your Key #s. Typically, you would have only one master area for each of these keys and the Key # would be 1. It is, however, possible that you have more that one PPK master area. For instance, you may have PPK Key # 1 for guest rooms and PPK # 2 for back of house doors. The Key # is important to use for the following reasons:
- When you make PPK & SPK keys, you must enter the Key #.
- When you interrogate a lock, the Key # will be printed. PPK & SPK keys are used with E2 Erase and LED Diagnostic keys and the lock will log the PPK or SPK key that was used.
- When you have more than one key for a master level (such as several different PPK keys), you will need to write the Key # on the key so employees will know in which rooms it works.

PPK & SPK ID #s: When you make PPK & SPK keys, the computer system automatically assigns a unique ID # between 1 and 255 to the key. For instance, you may have four copies of a PPK #1 key (one for each person who needs one) and they will have ID #s 1, 2, 3 and 4. When you first make keys, the computer begins with ID # 1. The ID # is important for the following reasons:
- When you interrogate a lock, the particular ID # used will be printed. This allows you to determine who used the PPK or SPK key. These keys are used with E2 Erase and LED Diagnostic keys and the lock will log the PPK or SPK key that was used.
- If you need to replace a worn out or expired key, you must enter the ID # when you duplicate the key.
- When you are assigning keys to departments instead of individual employees, you will need to write the ID # on the key so the department can track which ID # an employee signed out.

PPK & SPK Expiration: When you make PPK & SPK keys, you can enter the # of days you want the key to work for each ID#. You can choose from 0 to 999 days. If you enter 0, the key will expire (stop working in the locks) at the end of the day you make it. If you choose a number greater than 0, it will expire that many days from the day you make it. When you first make keys, the computer system will prompt you with a default # of days. When you make additional keys, the computer system will prompt you with the # of days that corresponds to the longest key expiration of the other IDs that you have already made for that master key.

7.2.2 Issuing and Controlling Special Keys

Establishing Master Key Control Sheets
The PPK & SPK keys should be recorded on the same control record for master keys (see Section 5.2.2).
- PPK or SPK level
- Key #
- ID #
- the name of the person or department that was given the key
- sign out & sign in times (if keys are signed out by different people)

When you need to replace a worn out or expired PPK or SPK key, you can verify the key's ID# using the control form.
When you interrogate a lock, you can refer to your control sheets to match the level, Key # and ID# with the person it was assigned to.

Labeling Special Keys when You Make Them
In order to be able to identify the special keys after you have made them, you will want to mark each key with the type of key it is (PPK, SPK E2 Erase, etc.). For PPK & SPK keys, you will also want to mark the Key # and ID#. You can use a permanent marker, labels or another suitable marking device.

If you use labels, do not put them on the keys until after you make each key and be sure to apply them to the lower half of the key. This is important to ensure the label cannot get stuck in the lock and will not interfere with encoding the key.

If you use a permanent marker, you can label the keys before you make them. You should write on the top half of the key so the marking will not wear off. You can also write on the bottom half of the key and then cover the writing with clear tape. If you use tape, always write on the bottom half of the key so the tape will not interfere when the key is inserted in the locks.

If you wish to punch a hole in the keycard to use it on a key ring, put the hole in the lower portion of the card.

Signing Out PPK & SPK Keys
If any employees will sign out PPK or SPK keys, be sure to establish a control sheet and procedures to ensure you will have a record of who had access to them. You may also want the person to sign their name or initials. The keys you use for signing out should be different than the ones permanently assigned to employees. In other words, they should have their own ID# so there is no possibility of confusing who had the key at any time. When a lock is interrogated, you will be able to identify the "sign out" keys and use the control sheet to determine who had the key at that time.

7.2.3 Initially Making All Your Special Keys

When you first receive your computer system, you will need to make all your special keys.

Step 1. First determine who will need keys and set up your control sheets for the PPK & SPK keys (see Section 7.2.2). You do not need control sheets for the E2 Erase, LED Diagnostics or Display keys.

Step 2 You should now mark or prepare your key labels (see Section 7.2.2). If you use a permanent marker to label your keys, you should mark each key you will make. If you use labels, you should make the labels, but do not apply them to the keys. Keep in mind that the PPK and SPK key ID#s will start at ID# 1.

Step 3 Follow the procedures in Section 7.3 MAKING SPECIAL KEYS. If you use labels on your keys, you should apply the appropriate label after you make each key.

If you are interrupted while making keys and do not make all the keys at once, simply re-enter the function to continue.

Step 4 Once the keys are made, you need to distribute them to the appropriate people. It is not necessary to use the new keys in all the locks since there are no old master keys.

7.2.4 Replacing Damaged, Lost or Expired Keys

If you need to replace a damaged, worn out, lost or expired key, you will simply re-encode the one key. If a special key is lost or stolen, you DO NOT need to replace any keys except the lost or stolen keys since no special keys can open doors.

Step 1. For PPK and SPK keys, you will need to know and enter the ID#s of the keys when you re-make them. If you do not have the key type, key # and/or ID# written on the keys, refer to your control sheets (see Section 7.2.2).

Step 2 If you are re-making keys that have expired, you can simply re-encode them. If you are replacing worn out keys, you should now mark or prepare your key labels (see Section 7.2.2). If you use a permanent marker to label your keys, you should mark each key you will make. If you use labels, you should make the labels, but do not apply them to the keys until after the keys are encoded.

Step 3 Follow the procedures in Section 7.3 MAKING SPECIAL KEYS. If you are re-making PPK or SPK keys, you will need to enter the ID # you are re-making.

Step 4 Once the keys are made, you should destroy any original worn out keys so there is no possibility they will still work. You can then distribute the re-made keys to the appropriate persons. It is not necessary to use the keys in the locks.

7.2.5 Making Additional Special Keys for Additional Employees

Step 1. If you are making additional PPK or SPK keys, first update your control sheets (see Section 7.2.2) for the new ID# keys. The keys you make will have the next ID#.

Step 2 You should now mark or prepare your key labels (see Section 7.2.2). If you use a permanent marker to label your keys, you should mark each key you will make. If you use labels, you should make the labels, but do not apply them to the keys until after the keys are encoded.

Step 3 Follow the procedures in Section 7.3 MAKING SPECIAL KEYS. If you are re-making PPK or SPK keys, you will need to enter 0 instead of an ID # to generate additional ID #s.

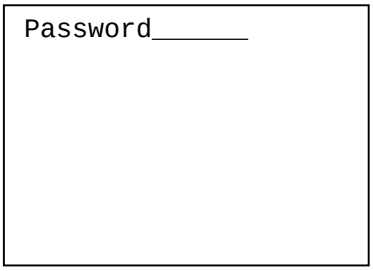
Step 4 Once the keys are made, you need to distribute them to the appropriate people. It is not necessary to use the keys in the locks since they are duplicates of the existing keys.

7.3 MAKING SPECIAL KEYS

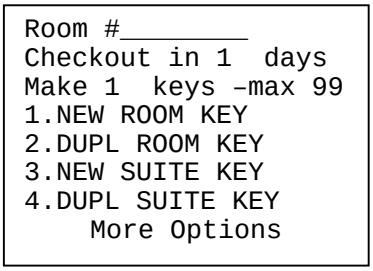
7.3.1 Selecting the Miscellaneous Keys Menu Function

To make any of the special keys, you can follow these steps to display the Miscellaneous Keys Menu.

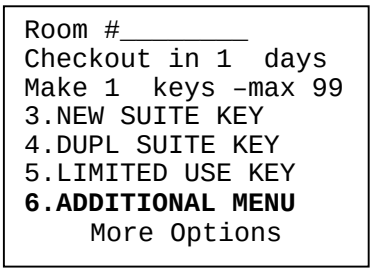
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



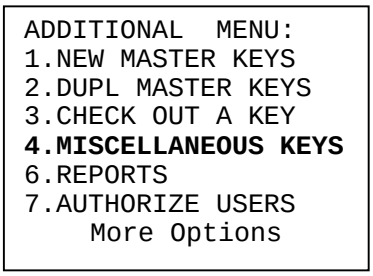
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 6 or use the ARROW DOWN key to display 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 4 or use the ARROW DOWN key to display the 4.MISCELLANEOUS KEYS menu item. Then press ENTER.



Step 5. The following MISC KEYS MENU screen will appear. You can now select the type of key you want to make or press ESC to return to the Sign On screen. Refer to sections 7.3.2 through 7.3.5 for the additional key making steps.

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

7.3.2 Making PPK Keys

You can make up to 255 PPK keys with different ID#s. PPK keys will expire, but there is no such thing as a new PPK key that will cancel out previously made PPK keys.

Step 1. Follow the steps in Section 7.3.1 to select the MISC KEYS MENU function. The MISC KEYS MENU screen will then appear.

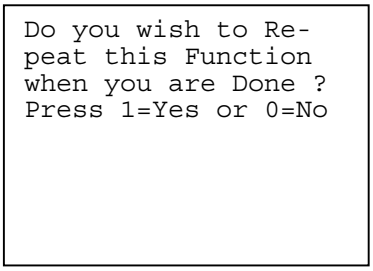
Step 2. At the MISC KEYS MENU screen, press 1 or use the ARROW key to select 1.PPK KEYS, then press ENTER. Or you can press ESC to end key making and return to the Sign On screen.

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

Step 3. The miscellaneous key number(s) will display. Select the number associated to the required key to make.

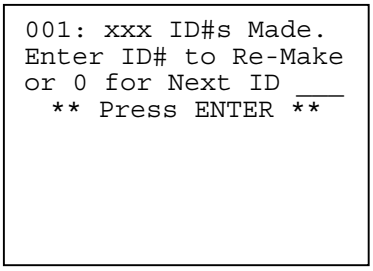
```
Select Master Key:
1. 1




Enter 1-1 (0=More)__
```

Step 4. The following screen will now appear. If you are making many different special keys, we suggest you press 1. If you do, you will return to the MISC KEYS MENU screen after you make keys instead of returning all the way back to the Sign On screen.

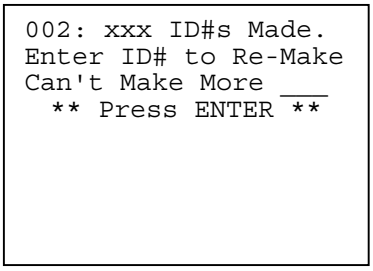


Step 5. If you are authorized for 1.All Auths or 5.Master keys, one of the following screens will then appear.
If you have made less than 255 different key ID#s, you will get screen 001.
If you entered a Key ID# to re-make from Screen 001 and made the key, you will next get screen 002.
If you have already made 255 different key IDs, you will also get screen 002.

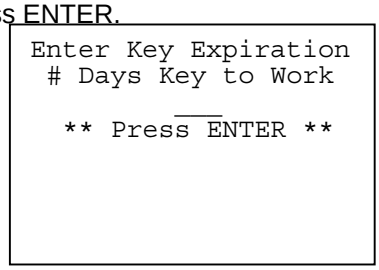
If screen 001 is displayed, the # of key ID#s made so far is indicated on the 1st line. You can make additional keys (with new key ID#s) or you can enter an existing key ID# to replace an existing key. If you want to make more keys to distribute to additional people, enter 0 and press ENTER. If you want to re-make a worn out or expired key, enter the key ID # of the key you want to replace and press ENTER.



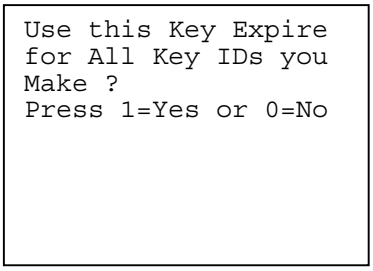
If screen 002 is displayed, you are only allowed to re-make existing key IDs. Enter the key ID # of the worn out or expired key you are re-making and press ENTER.



Step 6. The following screen will then appear. Enter the # of days you want the key to work. If you enter 0 days, the key will expire at the end of the day. You will notice that a default value is provided. If all your previously made keys have expired, the default value displayed will be 511 days. Otherwise, the default will be the longest # of days that your previously made keys will work. For example if you made a key that would work for 5 days and then made another that would work for 100 days, the screen would show 100 days as the default. You can, however, change it to anything from 0 to 999 days by simply entering the new value. Then press ENTER.



Step 7. The following screen will then appear. If you want all the keys you are going to make to have the same key expiration that you entered in step 6, press 1 then ENTER. If you want to enter a different # of days for each Key ID# to work, press 0 then ENTER.

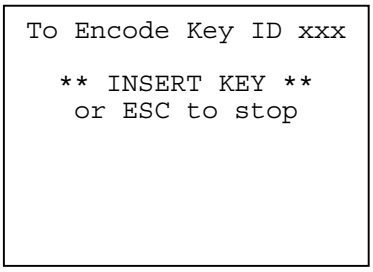


Step 8. The screen instructing you to insert a key should now appear. The Key's ID # is shown on the 1st line (from 1 to 255). Be sure to record this number on the keycard. When you distribute the keys, you will want to assign a person's name to the key ID# you give them. If you interrogate locks later, you will then be able to determine who used the key by its ID#.

After you make the key:
If you entered a Key ID# to re-make in step 5, you will return to Step 5 so you can choose a different key ID #.

If you pressed 0 in step 7, you will return to Step 6 so you can choose a different key expiration.

Otherwise, this screen will reappear after you make each key ID. Make the number of keys you will want to distribute and then press ESC to end key making.



Step 9. If you press ESC or time out at any point after step 4, the transaction will end.

If you indicated 1=Yes in Step 4, you will now return to the MISC KEYS MENU screen (Section 7.3.1 step 4) and can select other special keys to make.

If you indicated 0=No in Step 4, you will now return to the Password/Sign On screen.

7.3.3 Making SPK Keys

You can make up to 255 SPK keys with different ID#s. SPK keys will expire, but there is no such thing as a new SPK key that will cancel out previously made SPK keys.

Step 1. Follow the steps in Section 7.3.1 to select the MISC KEYS MENU function. The MISC KEYS MENU screen will then appear.

Step 2. At the MISC KEYS MENU screen, press 4 or use the ARROW DOWN key to select 4.SPK KEYS, then press ENTER.

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

Step 3. The miscellaneous key number(s) will display. Select the number associated to the required key to make.

```
Select Master Key:
1. 1




Enter 1-1 (0=More)__
```

Step 4. The following screen will now appear. If you are making many different special keys, we suggest you press 1. If you do, you will return to the MISC KEYS MENU screen after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 5. If you are authorized for 1.All Auths or 5.Master keys, one of the following screens will then appear.
If you have made less than 255 different key ID#s, you will get screen 001.
If you entered a Key ID# to re-make from Screen 001 and made the key, you will next get screen 002.
If you have already made 255 different key IDs, you will also get screen 002.

If screen 001 is displayed, the # of key ID#s made so far is indicated on the 1st line. You can make additional keys (with new key ID#s) or you can enter an existing key ID# to replace an existing key. If you want to make more keys to distribute to additional people, enter 0 and press ENTER. If you want to re-make a worn out or expired key, enter the key ID # of the key you want to replace and press ENTER.

```
001: xxx ID#s Made.
Enter ID# to Re-Make
or 0 for Next ID ___
  ** Press ENTER **
```

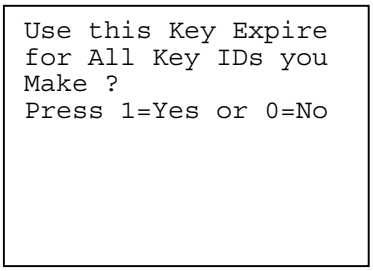
If screen 002 is displayed, you are only allowed to re-make existing key IDs. Enter the key ID # of the worn out or expired key you are re-making and press ENTER.

```
002: xxx ID#s Made.
Enter ID# to Re-Make
Can't Make More ___
  ** Press ENTER **
```

Step 6. The following screen will then appear. Enter the # of days you want the key to work. If you enter 0 days, the key will expire at the end of the day. You will notice that a default value is provided. If all your previously made keys have expired, the default value displayed will be 511 days. Otherwise, the default will be the longest # of days that your previously made keys will work. For example if you made a key that would work for 5 days and then made another that would work for 100 days, the screen would show 100 days as the default. You can, however, change it to anything from 0 to 999 days by simply entering the new value. Then press ENTER.

```
Enter Key Expiration
 # Days Key to Work
        ___
  ** Press ENTER **
```

Step 7. The following screen will then appear. If you want all the keys you are going to make to have the same key expiration that you entered in step 6, press 1 them press ENTER. If you want to enter a different # of days for each Key ID# to work, press 0, then press ENTER.



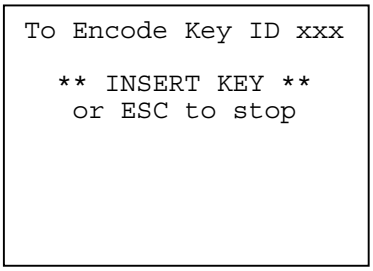
Step 8. The screen instructing you to insert a key should now appear. The Key's ID # is shown on the 1st line (from 1 to 255). Be sure to record this number on the keycard. When you distribute the keys, you will want to assign a person's name to the key ID# you give them. If you interrogate locks later, you will then be able to determine who used the key by its ID#.

After you make the key:

If you entered a Key ID# to re-make in step 5, you will return to Step 5 so you can choose a different key ID #.

If you pressed 0 in step 7, you will return to Step 6 so you can choose a different key expiration.

Otherwise, this screen will reappear after you make each key ID. Make the number of keys you will want to distribute and then press ESC to end key making.



Step 9. If you press ESC or time out at any point after step 4, the transaction will end.

If you indicated 1=Yes in Step 4, you will now return to the MISC KEYS MENU screen (Section 7.3.1 step 4) and can select other special keys to make.

If you indicated 0=No in Step 4, you will now return to the Password/Sign On screen.

7.3.4 Making E2 Erase & LED Diagnostic Keys

You can make any number of E2 Erase and LED Diagnostics keys. These keys require a valid PPK or SPK when they are used so they do not have different ID#s and they do not expire.

Step 1. Follow the steps in Section 7.3.1 to select the MISC KEYS MENU function. The MISC KEYS MENU screen will then appear.

Step 2. At the MISC KEYS MENU screen, press 2 or use the ARROW DOWN key to select 2.STATUS KEYS, then press ENTER. Or you can press ESC to end key making and return to the Sign On screen.

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

Step 3. The following screen will now appear. If you are making many different special keys, we suggest you press 1. If you do, you will return to the MISC KEYS MENU screen after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 4. If you are authorized for 1.All Auths or 5.Master keys, the following menu screen will then appear.

To make an LED Diagnostics key, press 1, then press ENTER.

To make an E2 Erase key, press 3 or use the ARROW DOWN key, then press ENTER.

```
SELECT STATUS KEY
1.LED Diagnostic
3.E2 Erase
```

Step 5. The screen instructing you to insert a key should now appear. Be sure to mark the keys you make as either LED Diagnostic or E2 Erase keys. This screen will reappear after you make each key. Make the number of keys you will want to distribute and then press ESC to end key making.

```
To Encode Key

** INSERT KEY **
 or ESC to stop
```

Step 6. If you press ESC in step 5, one of the following screens will appear. If you had not made any keys, you will get the first message. If you made some keys, you will get the second message and it will tell you the # of keys you just made.

```
M250: NO KEYS MADE
Make more Status
Keys ?
Press 1=Yes or 0=No
```

```
M251: xxx KEYS MADE
Make more Status
Keys ?
Press 1=Yes or 0=No
```

If you wish to return to step 4 and make a different type of key, press 1. You will then return to step 4.

If you are done making keys, press 0. If you timed out at any step in this function or you indicate 0=No in the screen, the transaction will end and you will return to the Password/Sign On screen.

Step 7. If you press 0 in step 6, the transaction will end.

If you indicated 1=Yes in Step 3, you will now return to the MISC KEYS MENU screen (Section 7.3.1 step 4) and can select other special keys to make.

If you indicated 0=No in Step 3, you will now return to the Password/Sign On screen.

7.3.5 Making Display Keys

You can make any number of Display keys. Since these keys do not affect the lock when they are used, they do not have different ID#s and they do not expire.

Step 1. Follow the steps in Section 7.3.1 to select the MISC KEYS MENU function. The MISC KEYS MENU screen will then appear.

Step 2. At the MISC KEYS MENU screen, press 3 or use the ARROW DOWN key to select 2.DISPLAY KEYS, then press ENTER. Or you can press ESC to end key making and return to the Sign On screen.

```
MISC KEYS MENU
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEYS
4.SPK KEYS
```

Step 3. The following screen will now appear. If you are making many different special keys, we suggest you press 1. If you do, you will return to the MISC KEYS MENU screen after you make keys instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 4. If you are authorized for 1.All Auths or 5.Master keys, the following menu screen will then appear. To make the Display key you want, press the # of the menu item or use the ARROW DOWN key to highlight the selection. Then press ENTER.

```
SELECT DISPLAY KEY
1.EPROM Program Vers
2.Clock Time
3.Clock Date
4.Interrogation Key
6.Knob Switch Status
7.Dead Bolt Status
9.Low Battery Status
```

Step 5. The screen instructing you to insert a key should now appear. Be sure to mark the keys you make for the type of Display key you selected. This screen will reappear after you make each key. Make the number of keys you will want to distribute and then press ESC to end key making.

```
To Encode Key

** INSERT KEY **
 or ESC to stop
```

Step 6. If you press ESC in step 5, one of the following screens will appear. If you had not made any keys, you will get the first message. If you made some keys, you will get the second message and it will tell you the # of keys you just made.

```
M250: NO KEYS MADE
Make more Status
Keys ?
Press 1=Yes or 0=No
```

```
M251: xxx KEYS MADE
Make more Status
Keys ?
Press 1=Yes or 0=No
```

If you wish to return to step 4 and make a different type of key, press 1. You will then return to step 4.

If you are done making keys, press 0.

Step 7. If you press 0 in Step 6, the transaction will end.

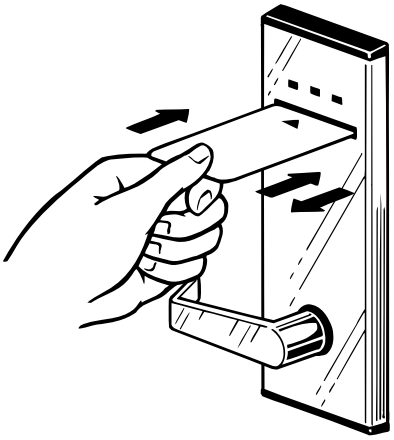
If you indicated 1=Yes in Step 3, you will now return to the MISC KEYS MENU screen (Section 7.3.1 step 4) and can select other special keys to make.

If you indicated 0=No in Step 3, you will now return to the Password/Sign On screen.

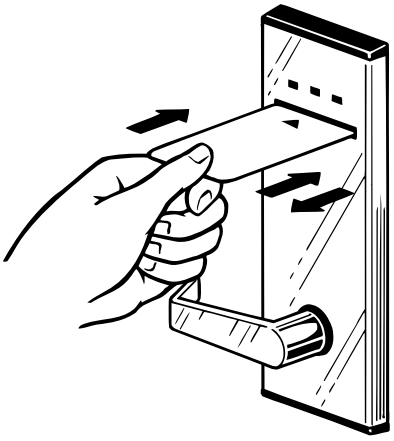
7.4 USING PPK & E2 ERASE KEYS TO ERASE A LOCK

This procedure will completely erase a lock. When a lock is erased, it goes into Mode 1 and no keycards will work until it is programmed again. Refer to Section 14.5.1 for an explanation of the Mode lights that keys will produce if a lock is in Mode 1. You will need the PPK key and an E2 Erase key.

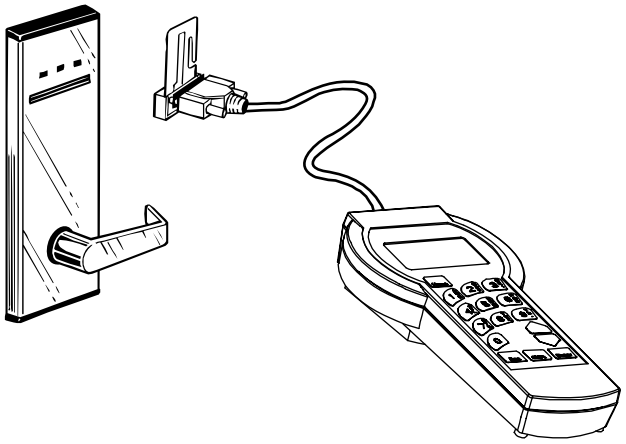
Step 1. Use the PPK key in the lock to get a slow flashing yellow light.



Step 2. While the light is flashing, use the E2 Erase key. About 2 seconds after the E2 Erase key is used, the yellow and green lights will flash together 2 times, then the yellow light will flash once.



Step 3. The lock is now in Mode 1 and ready to be programmed with a Hand-Held Terminal. If you use any keys before it is programmed, the lock will display Mode 1 lights - 1 green flash followed by all the lights flashing four times.



7.5 USING PPK & LED DIAGNOSTIC KEYS FOR LOCK DIAGNOSTICS

This procedure will allow you to turn a lock's LED Diagnostics feature on so you can determine why a key did not work in the lock. Refer to Section 14.5.2 for complete procedures for using LED Diagnostics. You will need the PPK or SPK key, the LED Diagnostics key and the key that did not work.

7.5.1 Turning LED Diagnostics On and Diagnosing Keys

Step 1. You must take the following keycards to the door:
- PPK or SPK key
- LED Diagnostics key
- the key or keys that did not work in the lock

Step 2. To turn the lock's diagnostics on, use the PPK or SPK key to get a slow flashing yellow light. While the yellow light is flashing, use the LED Diagnostics key. The lock's green and yellow lights should flash 3 times, indicating diagnostics has been turned on. LED diagnostics will stay on as long as you use keys (in step 3) within 2 minutes of each other.

Step 3. Now use the key that did not work in the lock. If the key is actually working normally, you will get the normal lights to indicate there is no problem. If the key did not work, the lock will flash the following lights. You must count how many times the green, yellow and red lights flash to determine the diagnostics code. If you lose track of the count, simply repeat this step again after the lights stop flashing.

- All lights flash together once (get ready to count)
- Count the # of times the Green light flashes (0 to 2)
- Count the # of times the Yellow light flashes (0 to 9)
- Count the # of times the Red light flashes (0 to 9)
- All lights flash together once (indicates it is done)

To turn the light counts into a diagnostic code, the green light count is the 100's digit, the yellow light count is the 10's digit and the red light count is the 1's digit. For instance, 1 green, 8 yellow and 6 red would be 186 and 1 green, 5 yellow and 0 red would be 150.

Step 4. To diagnose another key, repeat step 3.

Step 5. Refer to Section 14.5.2 for explanations and instructions for each the diagnostic codes.

7.5.2 Turning LED Diagnostics Off

When you are done diagnosing keys, you can turn LED Diagnostics off by using the LED Diagnostics key by itself. If you do not turn LED Diagnostics off, it will automatically turn off two minutes after the last key is used in it. You may get either of the following lights when you use the LED Diagnostics key. In either case, it indicates it is turned off.

If the LED Diagnostics key produces 3 flashes of the green and yellow lights, it indicates it turned it off.

If the LED Diagnostics key produces all lights flashing 4 times, it indicates that LED Diagnostics was already turned off.

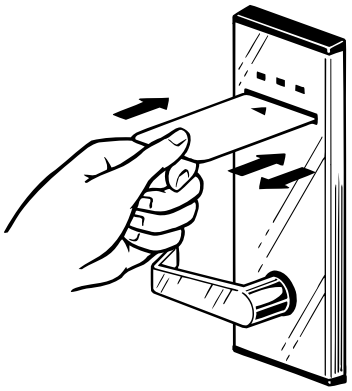
7.6 USING DISPLAY KEYS TO DISPLAY LOCK INFORMATION

Display keys are used to display various lock conditions through the lock's LED lights. They do not require any key to be used before them and they do not affect any keys working in the lock. The Lock Installation Manual refers to using these keys when installing a lock to test the hardware. Most often, however, a Display key is used to verify whether a lock is functioning if other keys produce no lights when they are used. Display keycards may include the following:

- Display EPROM Version (Lock's program version)
- Display Clock Time
- Display Clock Date
- Display Knob Turn Switch Status
- Display Dead Bolt/Privacy Switch Status
- Display Low Battery Status

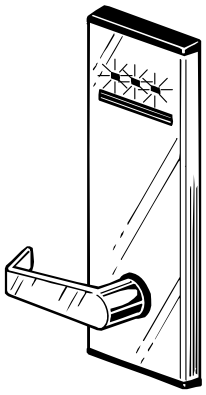
7.6.1 Using a Display Key in a Lock

Step 1. Use the Display key in the lock.

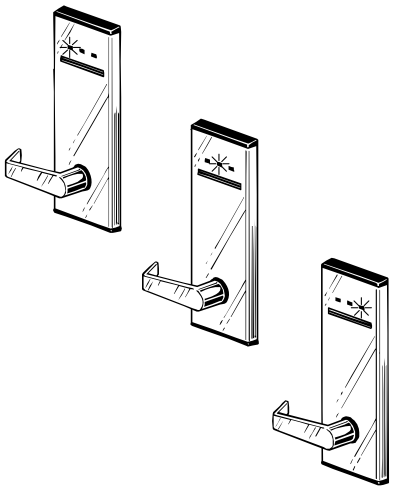


Step 2. You should then see all the lights come on for a second. Then you will get no lights or some combination of individual green, yellow then red flashes that you will want to count. These lights represent a number from 0 to 999.

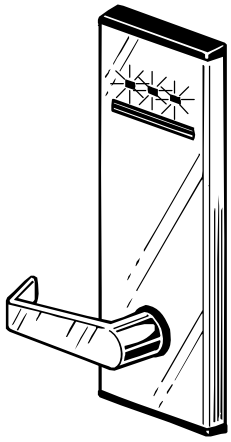
The # of times the green light flashes indicate the 100's value. The # of times the yellow light flashes indicate the 10's value and the # of times the red flashes indicates the 1's value. If no lights flash, the value is 0. Refer to the particular Display key you are using to determine what the count number represents.



Step 3. Depending on the type of Display key you used, step 2 may repeat several more times. When all the lights come on together, it indicates the end of one count and the beginning of another count. Refer to the particular display key you are using to determine how many different counts it displays and what each one is.



Step 4. When all the key's counts are finished, all the lights will come on again and then they will all go out. If you lose track of the counts, you can simply start over at Step 1 and use the key again.



7.6.2 The Various Display Keys

DISPLAY EPROM VERSION (LOCK'S PROGRAM VERSION)
This keycard displays the program version of the lock's EPROM chip. A total of 5 different counts will be displayed. The version includes a compatibility code, a version date and an application code.

	100'S Green	10'S Yellow	1'S Red
All lights			
COMPATIBILITY CODE (1-5)	-	-	X
All lights			
VERSION MONTH (1-12)	-	X	X
All lights			
VERSION DATE (1-31)	-	X	X
All lights			
VERSION YEAR (00-99)	-	X	X
All lights			
APPLICATION (1-9)	-	X	X
All lights			

DISPLAY CLOCK TIME

This keycard displays whether the lock's clock needs updating and the lock's current clock time. A total of 4 different counts will be displayed.

	100's Green	10's Yellow	1's Red
All lights			
CLOCK NOT SET PROBLEM (0-4)*	-	-	X
All lights			
DST STATUS (0=not DST or 1=DST)	-	-	X
All lights			
HOUR (0-23 Military Time)	-	X	X
All lights			
MINUTE (00-59)	-	X	X
All lights			

* The CLOCK NOT SET values indicate the following:
0 = No problem - clock is set.
1 = Lock is in Mode 0 or 1 - program lock.
2 = Lock needs DST information programmed in - update clock.
3 = Lock clock has reset - update clock.
4 = Lock clock has not been reset within 12 months - update clock.

DISPLAY CLOCK DATE

This keycard displays whether the lock's clock needs updating and the lock's current clock date. A total of 5 different counts will be displayed.

	100's Green	10's Yellow	1's Red
All lights			
CLOCK NOT SET PROBLEM (0-4)*	-	-	X
All lights			
DST STATUS (0=not DST or 1=DST)	-	-	X
All lights			
HOUR (0-23 Military Time)	-	X	X
All lights			
MINUTE (00-59)	-	X	X
All lights			

* The CLOCK NOT SET values indicate the following:
0 = No problem - clock is set.
1 = Lock is in Mode 0 or 1 - program lock.
2 = Lock needs DST information programmed in - update clock.
3 = Lock clock has reset - update clock.
4 = Lock clock has not been reset within 12 months - update clock.

DISPLAY KNOB TURN SWITCH STATUS

This keycard displays the current state of the lock's internal knob turn switch. It will allow you to test whether the turn switch, wire harness and connectors are working properly and the lock can sense when the handle is turned.

To test the knob turn switch, first open the door with a keycard and keep it opened. With the door opened, turn the inside handle and keep it turned while you use the Display key. You should get a single count (1 red) indicating that the handle is turned. Next, release the inside handle and use the key again. This time you should get no count (no lights) indicating the handle is not turned. If you do not get the correct counts, replace and return the exterior lock.

	100's Green	10's Yellow	1's Red
All lights			
KNOB TURN SWITCH STATUS (0-1)	-	-	X
(0 = Not turned, 1 = Turned)			
All lights			

DISPLAY DEAD BOLT/PRIVACY SWITCH STATUS

This keycard displays the current state of the lock's dead bolt or privacy switch. It will allow you to test whether the dead bolt / privacy switch, wire harness and connectors are working properly and the lock can sense when the dead bolt or privacy switch is activated is turned.

To test the switch, first open the door with a keycard and keep it opened. With the door opened, turn the dead bolt or turn the privacy switch. Then use the Display key. You should get a single count (1 red) indicating that the dead bolt or privacy feature is activated. Next, turn the inside handle to release the dead bolt / privacy switch and use the key again. This time you should get no count (no lights) indicating the dead bolt / privacy feature is not activated. If you do not get the correct counts, replace and return the exterior lock.

	100's Green	10's Yellow	1's Red
All lights			
DEAD BOLT SWITCH STATUS (0-1)	-	-	X
(0 = Not Activated, 1 = Activated)			
All lights			

DISPLAY LOW BATTERY STATUS

This keycard displays whether the lock's batteries are low and need replacing. This key will display two different counts. The first is a low battery flag and the second is the actual low battery status at the moment you use the key.

	100's Green	10's Yellow	1's Red
All lights			
LOW BATTERY STATUS (0-1)	-	-	X
(0 = No low indication, 1 = Low indication)			
All lights			
LOW BATTERY STATUS (0-1)	-	-	X
(0 = Not low now, 1 = Low now)			
All lights			

You would do different things depending on which combination of indications you get displayed.

Both = 0 This indicates no low battery problem.

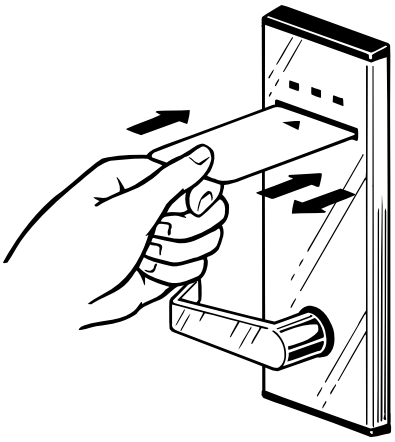
Flag = 1, Status = 0 This indicates that the last time a keycard opened the door, the batteries were low. If you have already replaced the batteries, you must use a key and open the door in order for the lock to clear the low battery flag. Then if you use this key, you will get a 0 count for both. If you have not replaced the batteries, this indicates that you should.

Both = 1 If the batteries are quite low, both counts will display a single red light. In this case, the batteries should be replaced immediately.

7.7 USING PPK OR SPK & MASTER KEYS TO ENTER A PROBLEM LOCK

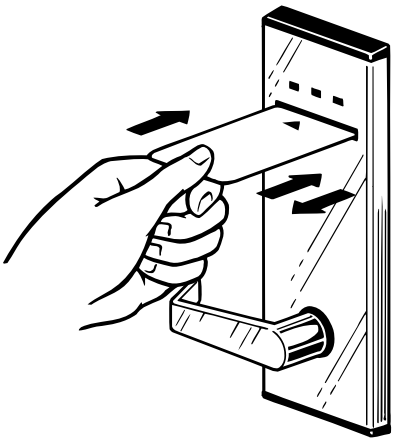
This procedure will allow you to enter a door if a lock goes into Mode 3 or Mode 5. Refer to Section 14.5.1 for an explanation of the Mode lights that keys will produce in Mode 3. You will need the PPK or SPK key and one or two different master keys. We would suggest using the Security/Emergency and the Grand Master key.

Step 1. Use the PPK or SPK key in the lock to get a slow flashing yellow light. Before you get the flashing yellow light, the Mode 3 or 5 lights will flash - Yellow and Green light twice and then all lights (Mode 3) or Yellow light twice and then all lights (Mode 5).

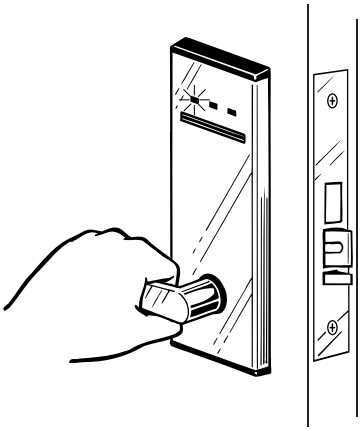


Step 2. While the yellow light is flashing, use the master key. If the key is current, the lock will flash the normal green light and you should open the door. A Mode 5 lock may have difficulty unlocking the door, so you should try steps one and two several times if the door does not initially open.

If you do not get the green flashing light, start over at Step 1 and use a different master level key in this step.



Step 3. Once you have the door open, you should not let it close until you are done troubleshooting and correcting the problem. If the lock is in Mode 3, replace the circuit board. If the lock is in Mode 5 replace the mortise. Refer to Section 14.5.1 and your Lock Installation manual for further troubleshooting procedures.



SECTION 8 - PROGRAMMING AND INTERROGATING LOCKS

8.1 PROGRAMMING LOCKS

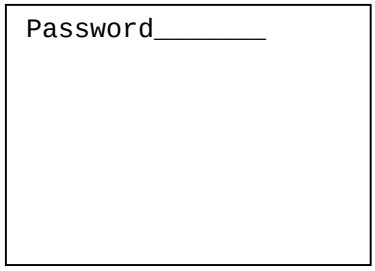
This function allows you to completely program or reprogram a lock by using an LPI/ELPS (Lock Programming / Interrogating) probe. It also instructs you how to program a lock by making and using Program keys if your LPI/ELPS probe is unavailable.

8.1.1 Programming Locks Using the LPI/ELPS Probe

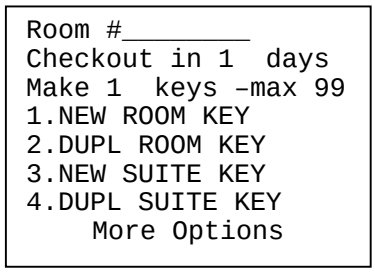
This function allows you to completely program or reprogram a lock using the Terminal and an LPI/ELPS probe. You will need an LPI/ELPS Probe to do this. If it is not available, you can follow the instructions in Section 8.1.2 Programming Locks Using Program Keys.
If you are not allowed to program a lock, the terminal will display an error screen to indicate why. If you cannot determine what is wrong, be sure to note all the information on the screen (particularly the error #).

SPARE DESKLINC COMPUTER: If you have a Spare DeskLinc Computer Terminal, you can use it to program locks, however, we do not recommend this. This is because it will not have current key data on the most recently made Master, Failsafe & Guest keys. This means that the lock will operate for old keys unless you use all the current master keys in it, use your 1st sequence of Failsafe keys and make New Room & Suite keys and use them in the lock after programming.

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 7 or use the ARROW DOWN key to display the 7.PROGRAM LOCK menu item. Then

press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
7.PROGRAM LOCKS
    More Options
```

Step 4. The following screen (Screen 010) should appear:

```
S010: SELECT OPTION
0.Not programming
1.Completely Program
2.Use ELPS to Unlock
or ESC to EXIT
```

Press 1, then press ENTER to completely program locks.

Step 5. The following screen (Screen 002) will appear. You must now enter the locks you want to program.

```
S002: Enter a Lock
You want to Program.
Room #: _____
Then Press ENTER or
ESC when finished
entering Room #s
```

Enter a room/lock # and press ENTER.

Step 6. The following screen will then appear.

```
M255: PLEASE WAIT
Requesting Data for
     Lock xxxxx
ESC to Abort Request
```

If you decide you did not want to program this lock, you can press ESC to abort the request. When the data is collected or you press ESC to abort the request, Screen 002 will reappear.

```
S002: Enter a Lock
You want to Program.
Room #: _____
Then Press ENTER or
ESC when finished
entering Room #s
```

Enter another lock and press ENTER or, if you are finished entering rooms, press ESC.

Step 7. The following screen (Message 254) will now appear:

```
M254: Disconnect
Terminal Cables and
  Connect LPI Probe
 ** PRESS ANY KEY **
```

Disconnect the RS232 Cable and power supply cord from the Hand-Held (and the printer cable if it is connected). Remove the Hand-Held Terminal from its base and connect the LPI/ELPS Probe to the printer port at the top of the terminal. Then press ANY KEY.

Step 8. The following menu screen (Screen 003) will now appear. You are now ready to take the Terminal and LPI/ELPS Probe to the door. You should also take a current Master key (such as the Security/Emergency key) with you since you will need it to open the door before programming.

```
S003: PROGRAM MENU 1
1.Program Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

Press ENTER if you want to completely program any locks. Go to step 9.
Press 3 and ENTER if you want to stop programming. Go to step 14.

Step 9. The following screen (Screen 005) will now appear. It will list all of the locks that you collected program data for and can use to program a lock. Although only up to 12 locks are displayed at a time, you can enter 0 to display any additional locks in the terminal.

```
S005: Program Lock:
1. 101     7. 107
2. 102     8. 108
3. 103     9. 109
4. 104    10. 110
5. 105    11. 111
6. 106    12. 112
Enter 1-12,0=more 0
```

Press the number (1-12) associated with the lock you want to program. Then press ENTER. If the lock you want is not displayed, press 0 and ENTER to display more locks. After selecting a lock, go to step 10. If you do not want to program any lock, press ESC and you will return to step 8.

Step 10. You should now use your master key to open the door. You should keep the door open until you are done programming the lock and are sure keys are operating in it.

If you have the LPI/ELPS probe connected, the following screen (Message 252) will now appear. Press any key and then insert the LPIprobe into the lock.

```
M252: Press Any Key
and THEN Insert LPI
  Probe into Lock!
(Press ESC to Abort)
```

Step 11. The terminal will then try to communicate with the lock, interrogate it and program it. While it is doing this, it will beep. If the terminal detects any reason why the lock cannot be programmed, it will display an error screens (refer to Section 13.5.5). If it is able to program the lock, it will continue to beep until it is done and then display the screen in step 12.

Step 12. After the lock is programmed, the following screen (Message 247) will appear. Press ANY KEY.

```
M247: LOCK xxxxx
   WAS PROGRAMMED
    SUCCESSFULLY
 ** PRESS ANY KEY **
```

Step 13. The terminal will then display the following screen (Message 243).

```
M243: REMOVE PROBE
   Press Any Key to
  Program More Locks
   or ESC to Stop
```

Remove the LPI/ELPS Probe from the lock. You should now use your master key to ensure the lock is working. If the key works, you can close the door. The programming process will inhibit all the currently issued Guest keys. If a guest is in the room, you will need to replace their key(s) with NEW keys.

Press ANY KEY if you want to program more locks. You will then return to step 9 for programming another lock.
Press ESC if you don't want to program more locks and return to step 8.

Step 14. When you are done programming locks and select item 3.RECONNECT TO STATION from the Screen 003 Program Menu 1, the following screen (Message 253) will appear:

```
M253: Disconnect LPI
Probe and Reconnect
Terminal Cables
** PRESS ANY KEY **
```

Disconnect the LPI/ELPS Probe from the Hand-Held. Replace the Hand-Held Terminal into its Base and reconnect the RS232 Cable and power supply cord (and Printer Cable if one is normally connected). Then press ANY KEY.

The following screens will appear to indicating the Terminal is re-establishing communications with its encoder.

```
M237: PLEASE WAIT
Terminal is Signing
Onto Station
*** ESC to Abort ***
```

<u>COMPUTER TERMINAL</u>
If you are using your main DeskLinc Computer Terminal and it is connected to its encoder, this will display very quickly and then proceed to Step 15.

If you are using your Spare DeskLinc Computer Terminal which does not have an encoder, you should press ESC at this screen. If you press ESC at the Message 237 screen, the Terminal will skip communications. You can then proceed to Step 15.

ADDITIONAL FRONT DESK TERMINAL

If you are using a Front Desk Terminal and it is connected to its encoder, the normal signing on messages will immediately begin displaying. If the DeskLinc Computer Terminal is on line, the 10 message collection screens will display and then proceed to Step 15.

```
SIGNING ONTO MAIN
     Requesting
System Date & Time
  ***Please Wait***
```

```
SIGNING ONTO MAIN
     Requesting
X of 10 Messages
***Please Wait***
```

Step 15. The following menu screen (Screen 004) will now appear:

```
S004: PROGRAM MENU 2
1.Exit Transaction
2.Collect Lock Data
3.Program More Locks
4.Make Program Keys
```

Press ENTER if you are done with all your programming and want to return to the Sign On screen.

Press 2 and ENTER if you want to collect lock data to program more locks. You will then need to follow steps 5 and 6. You will then return to this screen and can select menu item 3 to program the locks.

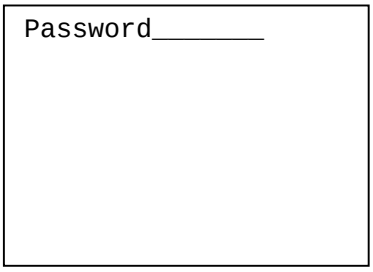
Press 3 and ENTER if you want to go program locks again. You will then return to step 7.

8.1.2 Programming Locks Using Program Keys

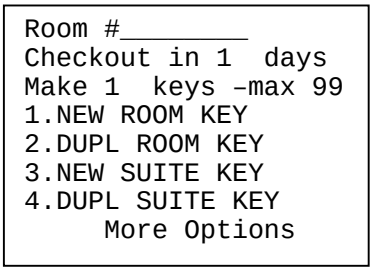
This function allows you to completely program or reprogram a lock using Program Keys made at a Terminal with an Encoder. It should only be done if you do not have an LPI/ELPS probe to use. If you are not allowed to make program keys, the terminal will display an error screen to indicate why. If you cannot determine what is wrong, be sure to note all the information on the screen (particularly the error #).

MAKING PROGRAM KEYS

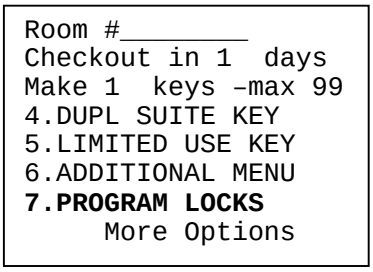
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



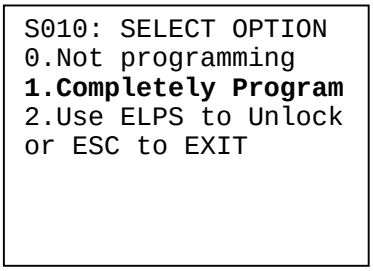
Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 7 or use the ARROW DOWN key to display the 7.PROGRAM LOCK menu item. Then press ENTER.



Step 4. The following screen (Screen 010) should appear:



Press 1 to completely program any locks.

Step 5. You must now enter the locks you want to make program keys for. The following screen (Screen 002) will appear:

```
S002: Enter a Lock
You want to Program.
Room #: _____
Then Press ENTER or
ESC when finished
entering Room #s
```

Enter a room/lock # and press ENTER.

Step 6. The following screen will then appear.

```
M255: PLEASE WAIT
Requesting Data for
     Lock xxxxx
ESC to Abort Request
```

If you decide you did not want to program this lock, you can press ESC to abort the request. When the data is collected or you press ESC to abort the request, Screen 002 will reappear.

```
S002: Enter a Lock
You want to Program.
Room #: _____
Then Press ENTER or
ESC when finished
Entering Room #s
```

Enter another lock and press ENTER or, if you are finished, press ESC.

Step 7. The following screen (Message 254) will now appear:

```
M254: Disconnect
Terminal Cables and
Connect LPI Probe
** PRESS ANY KEY **
```

YOU DO NOT NEED TO DISCONNECT any of the cables or connect the probe. Just press ANY KEY.

Step 8. The following menu screen (Screen 003) will now appear. Press 3 and ENTER to instruct the terminal to reconnect communications to its encoder.

```
S003: PROGRAM MENU 1
1.Program Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

Step 9. The following screen (Message 253) will appear:

```
M253: Disconnect LPI
 Probe and Reconnect
   Terminal Cables
 ** PRESS ANY KEY **
```

If you disconnected your cables in step 7, reconnect them. Then press any key.

Step 10. The following menu screen (Screen 004) will now appear. You can now make program keys for a lock, collect programming data for more locks or exit the function.

```
S004: PROGRAM MENU 2
1.Exit Transaction
2.Collect Lock Data
3.Program More Locks
4.Make Program Keys
```

Press 1 and ENTER if you are done making all your programming keys and want to return to the Sign On screen.

Press 2 and ENTER if you want to collect programming data for more locks to program. You will then need to follow steps 5 and 6. You will then return to this screen and can select menu item 4 to make Program Keys for the locks.

Press 4 and ENTER if you want to make Program keys for a lock. Then go to step 11.

Step 11. The following screen (Screen 005) will now appear. It will list all of the locks that you collected program data for and can use to make Program keys. Although only up to 12 locks are displayed at a time, you can enter 0 to display any additional locks in the terminal.

```
S005: Program Lock:
1. 101     7.107
2. 102     8.108
3. 103     9.109
4. 104    10.110
5. 105    11.111
6. 106    12.112
Enter 1-12, 0=more 0
```

Press the number (1-12) associated with the lock you want to make program keys for, then press ENTER. If the lock you want is not displayed, press 0 and ENTER to display more locks. After selecting a lock, go to step 12. If you do not want to make Program keys for any lock, press ESC and you will return to step 10.

Step 12. The following screen will now appear. You are being asked to enter the time that you will actually use the keys to program the lock. The terminal assumes that you will use the Program keys today so it assumes today's date. Whatever you enter here will be the time that the lock will actually program into its clock when you actually use the 5th Program key that you make in the lock.

```
S006:LOCK CLOCK TIME
Hour     (1-12) __
Mins     (0-59) __
AM (0) or PM (1) _
```

Enter the hour and press ENTER. Then enter the minutes and press ENTER. Then enter 0 for AM or 1 for PM and press ENTER.

Step 13. If the Terminal is still connected to its encoder, the following screen will now appear. You are now ready to make the keys. You will need to be prepared to make about 25 keys. Depending on the lock you chose, there could be less or more keys required.

BEFORE YOU START, IT IS IMPORTANT FOR YOU TO KEEP THE FOLLOWING IN MIND:
- You must keep the keys you make in the same order you make them. If they get out of order, the lock will not accept them when they are used.
- Each lock has different program keys. If you are making keys for more than one lock, it is imperative that you know which set of keys belong to which lock. Otherwise, you will program the lock to the wrong room # and keys. Mark the first key with the lock or room #.

```
    To Encode Key

** INSERT KEY **
 or ESC to stop
```

The screen will reappear after you make each key until the last key is made. REMEMBER TO KEEP THE KEYS IN ORDER AS YOU MAKE THEM.

If you do not make a key, the following screen will appear. To try again, press 1 and the Terminal will instruct you to insert a key again. If you press 0, the terminal will not try again and you should go to step 14.

```
E238: KEY # xxx FOR
LOCK nnnnn WAS NOT
MADE. Try Again ?
Press 1=Yes or 0=No
```

Step 14. If you did not make all the keys needed to completely program the lock in Step 13, the following screen will appear. If this message appears, press any key to return to step 11. You can then re-select the lock and start over. You should then re-encode any keys you have made.

```
E241: PROGRAM KEYS
  WERE NOT ALL MADE
   Do NOT Use Them.
 ** PRESS ANY KEY **
```

If you did make all the keys to program the lock, the following screen will then appear. It informs you that you must erase a lock before you can use the Program keys. You will need a PPK key that is currently working in the lock and an E2 Erase key in order to do this. Press any key to continue.

```
M239: YOU MUST USE
A PPK & E2 ERASE KEY
Before these Keys.
** PRESS ANY KEY **
```

The following screen will then appear. It informs you that the lock's clock will be set to the date and time displayed when you use the 5th Program key in the lock. If the date or time is not correct, you should re-select the lock and re-make the keys. Press any key to return to step 11. You can then select another lock or exit the transaction. Instructions for programming a lock are provided on the following pages.

```
M240: LOCK xxxxx's
CLOCK WILL BE set to
mm/dd/yy hh:mmx
** PRESS ANY KEY **
```

USING THE PROGRAM KEYS TO PROGRAM A LOCK

You will need a PPK key, the Security/Emergency key currently working in the lock, an E2 Erase key, the Program keys you made for the lock and a New room key you made for the lock. Since you had to enter a time that you would program the lock when you made the Program keys, you will want to wait until this time when you start step 5.

Step 1. Before going to the lock, you should make a New Room key for the room. After you are done programming the lock, you should use it to make sure you used the correct Program keys.

Step 2. Take all the keys to the lock. Use the Security key to open the door. You will want to keep the door open until you finish this procedure.

Step 3. To erase the lock, follow the instructions in Section 7.7 Using PPK & E2 Erase Keys to Erase a Lock. Once the lock is erased it will be in Mode 1. When you use any key, the lock will first flash the green light twice and then all lights at once. It will then flash other lights depending on the key you used. If you are unable to erase the lock, you cannot proceed with the remaining steps.

Step 4. Use the first 3 Program keys you made. The lock should display the following lights for each key:

- Use the 1st key. The lock should give you 2 Green flashes, then All lights then a slow flashing Yellow.
- While the lock is slowly flashing the yellow light, use the 2nd Program key. The lock should give you 2 Green and Yellow flashes and then the slow flashing Yellow again.
- While the lock is slowly flashing the yellow light, use the 3rd Program key. The lock should give you 2 Green and Yellow flashes and then the lights should go out.

Step 5. You can now use the remaining Program keys you made. You will want to do this step at the time that you indicated when you made the Program keys so that the lock will be programmed with the correct time. The lock should display the following lights for each key:

- Use the 4th key. The lock should give you a slow flashing Yellow.
- While the lock is slowly flashing the yellow light, use the next Program key. The lock should give you 2 Green and Yellow flashes and then the slow flashing Yellow again. If it does not, use the 4th key again to get the slow flashing yellow and then try again.
- When you are done using all the keys, the lock is completely programmed. If the yellow light is still flashing, use the 4th key again. The lock should give you All lights several times and then the lights should go out.

Step 6. You should now use the New Room key and be sure you can open the door. If it works, it indicates that you used the correct set of Program keys and can close the door. If it does not work, you should make sure the Security key will open the door before you let it close. You can then re-make the program keys and another New room key to try again.

Step 7. The Program keys you made should now be discarded or re-encoded so that they are not used again. If you wish to re-encode them, you can make use them to make New Room keys for room 71 (which is not a real room in your property) or to make Special Display keys which do not affect any locks (Section 7.3.5).

8.2 INTERROGATING LOCKS

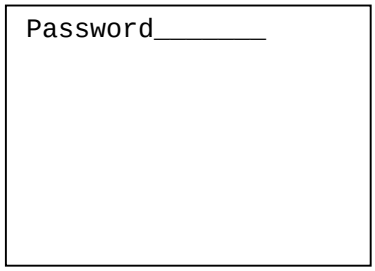
This function allows you to interrogate locks or update a lock's clock date and time. Refer to Section 8.3 for the procedure to update clocks. You will need an LPI/ELPS Probe to do these functions.

If you are not allowed to interrogate a lock, the terminal will display an error screen to indicate why. If you cannot determine what is wrong, be sure to note all the information on the screen (particularly the error #).

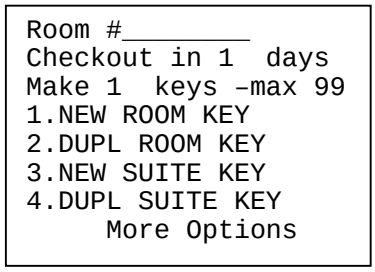
SPARE DESKLINC COMPUTER: If you have a Spare DeskLinc Computer Terminal, you can use it to interrogate locks, however, you should always make sure its System Date & Time and Daylight Savings Time information is correct before using it. Refer to Section 11 for instructions on doing this.

8.2.1 Interrogating Locks Using the LPI/ELPS Probe

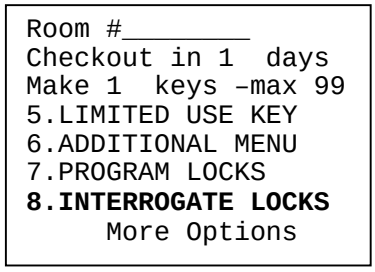
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 8 or use the ARROW DOWN key to display the 8.INTERROGATE LOCK menu item. Then press ENTER.



Step 4. The following screen (Message 254) will now appear:

```
M254: Disconnect
Terminal Cables and
Connect LPI Probe
** PRESS ANY KEY **
```

Disconnect the RS232 Cable from the Hand-Held (and the printer cable if it is connected). Remove the Hand-Held Terminal from its base and connect the LPI/ELPS Probe to the printer port at the top of the terminal. Then press ANY KEY.

Step 5. The following menu screen (Screen 003) will now appear:

```
S003: INTEROG MENU 1
1.Interrogate Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

Press ENTER if you want to interrogate a lock. Go to step 6.
Press 3 and ENTER if you want to stop interrogating locks. After you reconnect to the station, you will be able to print the interrogation reports. Go to step 10.

Step 6. If you have the LPI/ELPS probe connected, the following screen (Message 252) will now appear. Press any key and then insert the LPI probe into the lock.

```
M252: Press Any Key
and THEN Insert LPI
  Probe into Lock!
(Press ESC to Abort)
```

Step 7. The terminal will then try to communicate with the lock and interrogate it. While it is doing this, it will beep. If the terminal detects any reason why the lock cannot be interrogated, it will display an error screen (refer to Section 13.5.6). If it is able to interrogate the lock, it will continue to beep until it is done and then display the screen in step 8.

Step 8. After the lock is interrogated, the following screen (Message 247) will appear. Press ANY KEY.

```
M247: LOCK xxxxx
  WAS INTERROGATED
    SUCCESSFULLY
 ** PRESS ANY KEY **
```

Step 9. The terminal will then display the following screen (Message 243).

```
 M243: REMOVE PROBE
  Press Any Key to
Interrog More Locks
   or ESC to Stop
```

Remove the LPI/ELPS Probe from the lock.
Press ANY KEY if you want to interrogate more locks. You will then return to step 6.
Press ESC if you don't want to interrogate more locks and want to print the interrogations return to step 5. In step 5, you will want to select item 3.Connect to Station

Step 10. When you are done interrogating locks and select item 3.Connect to Station from the Screen 003 Interrogate Menu 1, the following screen (Message 253) will appear:

```
M253: Disconnect LPI
 Probe and Reconnect
   Terminal Cables
 ** PRESS ANY KEY **
```

Disconnect the LPI/ELPS Probe from the Hand-Held. Place the Hand-Held Terminal into the Base and connect the RS232 Cable and power supply cord (and Printer Cable if one is normally connected). Then press ANY KEY.

The following screens will appear to indicating the Terminal is re-establishing communications with its encoder.

```
M237: PLEASE WAIT
Terminal is Signing
    Onto Station
*** ESC to Abort ***
```

COMPUTER TERMINAL

If you are using your main DeskLinc Computer Terminal and it is connected to its encoder, this will display very quickly and then proceed to Step 11.

If you are using your Spare DeskLinc Computer Terminal which does not have an encoder, you should press ESC at this screen. If you press ESC at the Message 237 screen, the Terminal will skip communications. You can then proceed to Step 11.

ADDITIONAL FRONT DESK TERMINAL

If you are using a Front Desk Terminal and it is connected to its encoder, the normal signing on messages will immediately begin displaying. If the DeskLinc Computer Terminal is on line, the 10 message collection screens will display and then proceed to Step 11.

```
SIGNING ONTO MAIN
     Requesting
System Date & Time
  ***Please Wait***
```

```
SIGNING ONTO MAIN
     Requesting
X of 10 Messages
  ***Please Wait***
```

Step 11. The following menu screen (Screen 004) will now appear:

```
S004:INTERROG MENU 2
1.Exit Transaction
2.Print Lock Reports
3.Interrogate More
5.Read Inter. Card
```

Press ENTER if you are done with all your interrogating and printing and want to return to the Sign On screen.

Press 2 and ENTER if you have interrogated locks and want to print their reports. Go to step 12.

Press 3 and ENTER if you want to go interrogate locks again. You will then return to step 4.

Step 12. If you have interrogated locks, you will be able to select the menu item to print the reports. The following screens will appear if the System Printer is not assigned to your terminal.

```
E059: Printer Option
Must be To Terminal
Correct Option Now?
Press 1=Yes or 0=No
```

```
PRINTER CONNECTED
1.To Terminal
2.No Printer
```

Press 1 for Yes at the first screen then 1 then press ENTER to select 1. To Terminal at the second screen.

Step 13. Press ENTER to select 0 for Output Drain.

```
 Set Printer Output
      Type? 0
(0 = Output Drain)
(1= Totem Pole)
Press Enter or ESC
```

Step 14. After verifying the printer is connected and available, the following menu screen (Screen 006) will appear. It will list all the locks that you interrogated.

```
S006: Print Lock:
1. 103
2. 105



Enter 1-2, 0=more 0_
```

Press the number (1-2) associated with the lock you want to print. Then press ENTER. If the lock you want is not displayed, press 0 and ENTER to display more locks. After selecting a lock, go to step 15. If you do not want to print any more lock interrogations, press ESC and you will return to step 11.

Step 15. The following screen (Screen 007) will appear. You must now enter the # of days back you want the report to print. The default is 0 which means you want all the entries to print.

```
S007: For Lock xxxxx
Enter # of days back
to Print 0__ (0=all)
** ESC to Abort **
```

Press ENTER if you want the complete report.
Enter the # of days and press ENTER if you only want to go back a specific number of days.

Press ESC if you want to abort the report and return to step 14.
Step 16. You must now indicate if you want the entries to be adjusted to the terminal's date and time.

```
S009: For Lock xxxxx
Adjust Entries to
Terminal Date/Time?
Press 1=Yes or 0=No
```

Press 1 for Yes of 0 for No.

Step 17. The following screen will then appear.

```
238: PLEASE WAIT
Report on Lock xxxxx
is Printing
** ESC to Abort **
```

If you decide you did not want to print the report, you can press ESC to abort it. When the report is finished or you press ESC to abort it, Screen 006 will reappear. Return to step 14 to print additional interrogation reports.

```
S006: Print Lock:
1. 103
2. 105



Enter 1-2, 0=more 0_
```

Step 18. When finished printing reports, press ESC at the Print Lock screen. The screen will return to the Interrogation Menu 2. Press 1 then press Enter for Exit Transaction to return to the Sign On screen.

```
S004:INTERROG MENU 2
1.Exit Transaction
2.Print Lock Reports
3.Interrogate More
5.Read Inter. Card
```

See Section 8.2.6 for information on reading the lock interrogation report.

8.2.2 Interrogating Locks Using A Memory Keycard

The DeskLinc system will allow a lock to be interrogated with a memory keycard as well as with the hand-held and probe. Interrogating a lock with a memory keycard is best used if only recent key usages for a lock are required. A memory keycard will interrogate one lock.

Required Equipment

1. DeskLinc system with a memory keycard encoder
2. Saflok memory keycard
3. Locks with memory keycard readers
4. Printer

About Memory Keycards

Memory size (bits)	Interrogation Records	Part#
8KB	60	10380
64KB	172	10370

Interrogation Process

1. Making the interrogation key
2. Using the interrogation key in lock
3. Reading the interrogation key
4. Printing the interrogation report

8.2.3 Making the Interrogation Key

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

```
Password__________
```

Step 2. Press ENTER three times to move the cursor to the transaction menu.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
1.NEW ROOM KEY
2.DUPL ROOM KEY
3.NEW SUITE KEY
4.DUPL SUITE KEY
     More Options
```

Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
     More Options
```

Step 4. Press 4 or use the ARROW DOWN key to display the 4. MISCELLANEOUS KEYS item. Press ENTER

```
ADDITIONAL  MENU:
1.NEW MASTER KEYS
2.DUPL MASTER KEYS
3.CHECK OUT A KEY
4.MISCELLANEOUS KEYS
6.REPORTS
7.AUTHORIZE USERS
     More Options
```

Step 5. Press 3 or use the ARROW DOWN key to display the 3. DISPLAY KEYS item. Press ENTER

```
MISC KEYS MENU:
1.PPK KEYS
2.STATUS KEYS
3.DISPLAY KEY
4.SPK KEYS
```

Step 6. Press 0 for No if you are making one interrogation key or press 1 for Yes if you wish to make more than one key.

```
Do you wish to Re-
peat this function
when your done ?
Press 1=Yes or 0=No
```

Step 7. Press 4 or use the ARROW DOWN key to display the 4. Interrogation Key. Press ENTER.

```
SELECT DISPLAY KEY
1.EPROM Program Vers
2.Clock Time
3.Clock Date
4.Interrogation key
6.Knob Switch Status
7.Dead Bolt Status
9.Low Battery Status
```

Step 8. The screen instructing you to insert a key should now appear. Be sure to mark the key.

```
    To Encode Key

  ** INSERT KEY **
   or ESC to stop
```

Step 9. If 0 for No was selected in step 6 the screen will return to the Sign On screen. If 1 for Yes was selected, the following screen will appear.

```
M251:  1  KEYS MADE
Make more Display
Keys?
Press 1= Yes or 0=No
```

If you would like to make additional keys press 1 and return to step 7. Or Press 0 for No and then ESCAPE 2 times to return to the password screen.

8.2.4 Using the Interrogation Key in the Lock

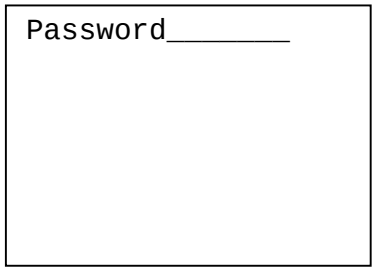
Step 1. Insert key into a lock with the memory-chip in the upward position.

Step 2. Hold the key inside the lock until a solid green light appears. The green light should come on with in a couple of seconds.

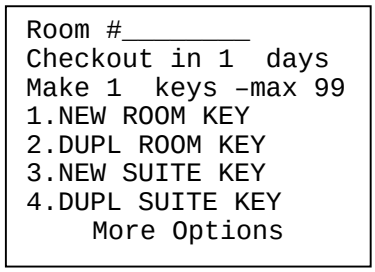
Step 3. Remove the key from the lock immediately after the green light appears. At this point the lock has been interrogated successfully.

8.2.5 Reading the Interrogation Key

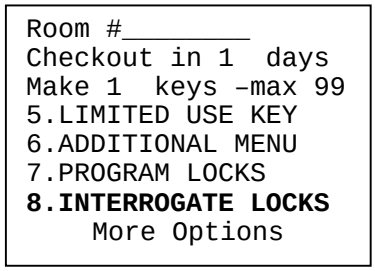
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



Step 2. Press ENTER three times to move the cursor to the transaction menu.



Step 3. Press 8 or use the ARROW DOWN key to display the 8.INTERROGATE LOCK menu item. Then press ENTER.



Step 4. The following screen (Message 254) will now appear:

```
M254: Disconnect
Terminal Cables and
Connect LPI Probe
** PRESS ANY KEY **
```

DO NOT disconnect the RS232 Cable from the Hand-Held (or the printer cable if it is connected) and do not connect the probe. Just press ANY KEY.

Step 5. Press 3 or use the ARROW DOWN key to display the 3. Connect to Station menu item. Then press ENTER.

```
S003: PROGRAM MENU 1
1.Interrogate Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

Step 6. The following screen (Message 253) will now appear:

```
M253: Disconnect LPI
Probe and Reconnect
   Terminal Cables
  **Press Any Key**
```

The probe is not connected and the terminal cable is still connected so simply press any key.

Step 7. Press 5. or use the ARROW DOWN key to display the 5. Read Inter. Card menu item. Then press ENTER.

```
S004:INTERROG MENU 2
1.Exit Transaction
2.Print Lock Reports
3.Interrogate More
5.Read Inter. Card
```

Step 8. Insert the memory keycard into the encoder when the below screen appears.

```
     To Read Key

  ** INSERT KEY **
   or ESC to stop
```

Step 9. Hold the key in the encoder while the below screen appears. The insertion slot on the encoder will illuminate solid green.

```
M250: Please wait

Interrogating Lock
 For Info Type 0
```

Step 10. Remove the key when the green lights flash around the insertion slot and the screen below appears. Then press ENTER.

```
M247: LOCK XXXXX
  WAS INTERROGATED
    SUCCESSFULLY
 ** PRESS ANY KEY **
```

Step 11. Press 2 or use the ARROW DOWN key to display the 2. Print Lock Reports menu item. Then press ENTER.

```
S004:INTERROG MENU 2
1.Exit Transaction
2.Print Lock Reports
3.Interrogate More
5.Read Inter. Card
```

Step 12. If you have interrogated locks, the following screen will appear. Connect the printer and its cable to the handheld. Then press ENTER.

```
M083:Connect Printer
to the Terminal and
    Press Any Key
 * or ESC to abort*
```

Step 13. After verifying the printer is connected and available, the following menu screen (Screen 006) will appear. It will list all the locks that you interrogated. Although only up to 12 locks can be displayed at a time, you can enter 0 to display any additional locks in the terminal.

```
S006: Print Lock:
1. 101
2. 103



Enter 1-2, 0=more 0_
```

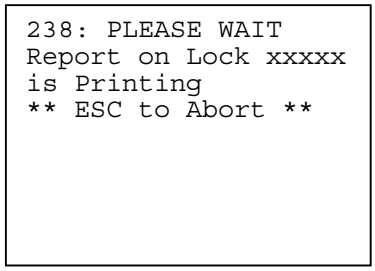
Press the number (1-12) associated with the lock you want to print. Then press ENTER. If the lock you want is not displayed, press 0 and ENTER to display more locks. After selecting a lock, go to step 14. If you do not want to print any more lock interrogations, press ESC and you will return to step 11.

Step 14. The following screen (Screen 007) will appear. You must now enter the # of days back you want the report to print. The default is 0 which will print all of the entries.

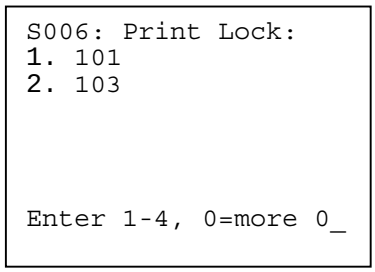
```
S007: For Lock xxxxx
Enter # of days back
to Print 0__ (0=all)
 ** ESC to Abort **
```

Press ENTER if you want the complete report.
Enter the # of days and press ENTER if you only want to go back a specific number of days.
Press ESC if you want to abort the report and return to step 11.

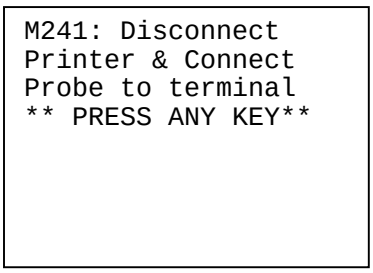
Step 15. The following screen will then appear.



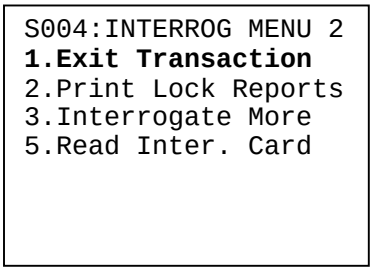
Step 16. After the report has finished printing, Screen S006 will reappear. Return to step 13 if you would like to print another lock interrogation report. If you do not want to print another interrogation report press ESC quit then continue to step 16.



Step 17. If your printer is normally connect to the terminal Press ENTER. Otherwise only disconnect the printer cable then press ENTER.



Step 18. Press 1 for menu item 1. Exit Transaction. Press ENTER. The terminal will return to the Password screen.



8.2.6 Reading the Lock Interrogation Report

Lock Interrogation Report - Sample Report

Below is a sample of the Lock Interrogation Report. Explanations of how to read it are provided on the following pages.

```
PAGE 1     06-29-2006  03:00PM DST    DESKLINC SYSTEM           TERMINAL # 1

LOCK STATUS REPORT:   REPORT # 2
-------------------------------------------------------------------------------
INTERROGATION FOR LOCK #: 101     PROPERTY#: 100    EPROM V: 6   04-08-2003.2

Report Date Format Used: MM-DD-YYYY   (Note: * is used if data is unavailable)

LOCK STATUS AT TIME OF INTERROGATION:
- Pattern: G  Checksum: G  Write: G  Mode: 2 - Property Prog'd
- E2 is Enabled
- Invalid Key Shutdown is not in effect
- Lock Batteries are Good
- Locked/Unlocked Switch - OK
- Key Switch - OK
- Intended to be Locked
- DST Change Info is set
DST is Standard U.S.
DST Starts 04-02 02:00  Ends 10-29 02:00  Year 2006
- Lock's Clock does not require resetting
- Lock uses Locked Switches? Y  Opening(Knob) Switch? Y
- Serial Port Communication:  Sends? N  Recvs? N
Lock's Clock Date & Time: 06-30-2006 12:18PM DST
Terminal's Date & Time: 06-30-2006 12:18PM DST
Lock Date & Time & DST Info was updated after 1st interrogation.

KEY USE & ENTRY RECORDS:
Key names are derived from:
NAMEINDX.ACT Vers: 04-24-2006
KEYPROG.ACT Vers: 03-21-2006

  1) LVL 01 TYPE 0: ROOM                       KEY  ID#: 2     KEY#: 101
From: Key  Used On:   06-29-2006 02:36PM DST,  Opened 1 Times

  2) LVL 08 TYPE 0: SECTION                    KEY  ID#: 4     KEY#: 11
From: Key  Used On:   06-29-2006 12:31PM DST,  Opened 1 Times

  3) LVL 01 TYPE 0: ROOM                       KEY  ID#: 1     KEY#: 101
From: Key  Used On:   06-29-2006 10:17AM DST,  Opened 1 Times
- New Key
```

Lock Interrogation Report - Information Explained

The report includes 4 sections. At the top is basic information on the lock interrogated. The next section prints lock status information. The third section prints basic information on the key uses and automatic logs. The last section prints each key use and lock status change from most to least recent.

INTERROGATION FOR LOCK #:
At the top of the report, the following information is provided:
Lock/room # - This is the lock name or room # interrogated.
Property # - This is the lock's property #. Locks programmed to your DeskLinc System will have your property #.
EPROM version - This is the software version of the lock's EPROM chip.
Date Format - This line indicates the format of all dates printed in the report (MM-DD-YY or DD-MM-YY)

LOCK STATUS AT TIME OF INTERROGATION:

This section of the report indicates the status of various lock hardware at the time of interrogation. It also provides date and time information. If you are having any problems, this information is often helpful in determining why.

Program Status - This line indicates if their were any errors in the lock memory storage chip (E2) and what Mode the lock was in. The Pattern, Checksum and Write error conditions should be "G", indicating good. The Mode # corresponds to the modes in Section 14.5.1. If the Mode is 2 - Property Programmed (and the lock's Property # matches yours), the lock will work normally for keys made by your DeskLinc System. If the Mode is 2 - Factory Programmed, the lock will work for Installation/New Construction keys.

E2 Chip Status - This indicates if the lock's memory chip (E2) is Enabled or Disabled. If it is Disabled, the lock will not allow any keys to work until it is Enabled again.

Invalid Key Shutdown Mode - This indicates if the lock is currently in this mode or not (Not in Effect or In Effect). If it is in effect, invalid keys will produce no lights. A valid key or waiting 2 minutes before using a key will cancel this mode.

Battery Status - This indicates the lock batteries are Good or Low. If they are low, you should change them.

Locking Switch Status - This only applies to locks with motors and indicates OK or Critical Locking Failure. If the lock has a Critical Locking Failure, it indicates that the motor is jammed or the motor position switches have a problem and the lock should be serviced.

Key Switch Status - This indicates whether the key switch is OK or Broken. If it indicates Broken, you should try using keys in the lock to see if the lock will read them. If they work, the key switch was simply activated just before you interrogated it. If they have trouble (no lights), you should replace the lock reader.

Intended Latch State - This indicates if the lock is currently intended to be Latched or Unlatched. Normally a lock should be Latched (locked & requiring keys to work). If a Latch/Unlatch key was used to unlatch it, it will also show in the log entries.

DST Information - This indicates if the lock is programmed for Daylight Savings Time changes and if so, when DST starts and ends. If the lock has no DST information, it will indicate Needs to be Reprogrammed. It can be reprogrammed by updating the lock's clock (Section 8.3).

Lock's Clock Status - This indicates whether the lock's will require you to periodically reset its clock. If it requires periodic resetting, it will indicate how many more months can pass before it will force you to reset it by displaying a red flashing light with the normal key lights. If it indicates it needs resetting now, you should update the lock's clock (Section 8.3).

Switches - This indicates whether the lock is programmed to look for motor locking switches (motor locks) and for a Knob turn switch (motor or solenoid locks). If the settings do not match the type of lock, it will not operate properly.

- A Motorized lock should have both "Y".
- A Solenoid lock should have Locking Switches "N" and Knob Switch "Y".
- ECUs and RCUs should have both "N".

If a lock has no Knob Switch, it cannot detect if a door is actually opened when a key is used. The key entry logs will always print "Opened 0 Times" in this case. (There is no knob switch related to turning the handle for ECUs and RCUs.)

Serial Port Communications - This indicates whether the lock communicates through its serial port to another device. All lock types should indicate "N".

Lock's Clock Date & Time - This indicates the lock's clock date and time when it was interrogated. If the lock is not sure of its accuracy, it will also print "Needs Updating" after it. If this is indicated, you should update the lock's clock (Section 8.3).

Terminal's Clock Date & Time - This indicates the Terminal's clock date and time when the lock was interrogated. It should be the same as or close to the lock's clock date and time. If it is not, you can determine the difference in time and add this time to the key entries to get a more accurate time of log entries.

Lock's Clock Date & Time Update - This indicates if the Terminal updated the lock's clock date & time after it interrogated it. If it was, any earlier settings indicating the lock's clock needed updating do not require you to update the lock's clock.

KEY USE & ENTRY RECORDS:

This section of the report indicates how the date & time for each entry record was determined and the version of the DeskLinc Computer's key design files that are used to print the Key # for each entry.

Report Days - If you requested a limited # of days to be printed, the report will indicate the range you chose. Otherwise, this line will not print.

Entry Dates & Times - This indicates the entry and other log dates printed were based on the lock's clock date & time when the entry occurred. They are not adjusted to reflect the Terminal's date & time. If the lock & terminal have different times (see previous section), you can adjust the entry dates and times for the difference.

Key Names - This information indicates that the key names or numbers were printed using the information from two of the Key Design files in the DeskLinc Computer. The version dates of the files are also provided.

KEY ENTRIES AND OTHER LOGS:

The remainder of the report details the key entries and other loggings that either changed the data stored in the lock or allowed the door to be opened. Each entry contains between 2 and 4 lines of information.

1ST LINE

This line identifies the key used or the automatic operation performed. Only keys that are valid actually log entries in the lock.

- Key Level and Type: These are code #s which are only used if the Description cannot be printed.
- Key or Log Description: This indicates the type of key used or a description of automatic logs that the lock performed. Typically, you will see Room, Floor, Security, etc. for keys. Another common one is PI Clock Key which indicates the lock's clock was updated.
  If Egress or Exit appears it indicates that the lock had a door-a-jar mortise and someone opened the door from inside the room and exited.
- Key ID # or User #: For normal keys (Room, Floor, Security, etc.), this indicates the key ID #. When duplicate keys exist, this identifies which one was used. To determine the actual person who used a master key, look up the key level, key # and ID# on your Master key control sheets (refer to section 5.2.2). If you program or interrogate a lock, the PPK key or LPI/ELPS Program key entry will instead print the user # of the person who used the Terminal. Refer to Section 9.1.6 to determine the name of the employee who has the user # printed.

2ND LINE

This line indicates what caused the log, date & time information and various other information based on what type of log it was.

- From: Indicates what generated the log entry:
  Key = key entries or programming keys from a Keycard
  LPI/ELPS = program or interrogation logs from an LPI/ELPS Terminal
  Lock = log of status changes automatically done by the lock
- Used On: or Occurred: Indicates the date & time the log occurred. For PI Clock Key logs, you will see New Date: or Orig Date: which indicate the lock's original date and time and the new date and time it was changed to.
- Allowed to Open: If these words appear, it indicates that the key used produced a green light and would allow the door to open. If these words do not appear, it indicates that a valid key was used but it did not allow the door to open. This could happen if the dead bolt or privacy switch was set, the door was electronically locked, or a guest key was used after the inhibit key.
  PPK, SPK and LPI/ELPS Program keys which do not open locks will log other information at the end of this line to indicate what other program keys were used with them. Other logs the lock does will usually indicate the status of the E2 memory chip before the log occurred. This is strictly trouble shooting information.

3RD LINE - OPTIONAL

- New Key: This indicates the key was a new key to the lock. It indicates this was the first time the new key was used in the lock.
- Was Dead Bolted: This indicates the lock was dead bolted or the privacy switch when the key was used and it was allowed to override the dead bolt or the privacy switch.
- Unlatched: This indicates the key was an Unlatch key which left the door in an unlatched state.
- Relatched: This indicates the key was an Latch key which left the door in a latched state.
- Elect Lock: This indicates the key was an Electronic Lockout key which left the door electronically locked
- Elect Unlock: This indicates the key was an Electronic Lockout key which left the door electronically unlocked.
- Inhibited: This indicates the key was an Inhibit key which inhibited all the current guest keys when it was used.
- Capabilities: This indicates the key was a PPK or SPK key and indicates which program authorizations the key had.

4TH LINE - OPTIONAL

This information will ONLY print if the following conditions occurred when the entry was logged:

- CLOCK NOT SET: This indicates the lock's clock was in need of updating when the log occurred and the date & time may not be accurate. The entry date & time can be verified from PI Clock Key logs that occurred after this entry.
- LOW BATTERIES: This indicates that the lock's batteries were low when the log occurred.
- LOCKING PROBLEM: This indicates that the lock was having a problem re-locking the door when the log occurred
- Lock Remains UNLATCHED: This indicates that the lock had been previously been unlatched on purpose by a Latch/Unlatch key and has not yet been re-latched. When a lock is left unlatched, the handle can be turned without using a key and without logging an entry.

Lock Interrogation Report - Examples of Special Log Entries Explained

While most log records on the report are obvious, there are certain combinations of entries that always represent certain things that were done to the lock. Generally, these combinations of logs indicate programming or interrogating the lock. Below are the log combinations that would indicate programming or interrogating occurred.

LOGS INDICATING A LOCK WAS COMPLETELY PROGRAMMED:
The following logs would be done when completely programming a lock. If you use an LPI/ELPS probe and terminal, all the entries will show From: LPI/ELPS. If you use program keys, all the entries will show From: Key. If you use Program keys or you use the LPI/ELPS and reprogrammed a lock from one room number to another, the lock will first be erased. If you simply reprogrammed a lock to the same room number with the LPI/ELPS, it would not be erased. Next, you will see a PPK key and an SPK key. You will then see the PPK key twice again. Lastly the logs show the two PI Clock Key logs indicating the clock date & time were updated. The first log shows the lock's original date and time and the second log shows the new date and time it was changed to. If you use the LPI/ELPS, all the keys indicate the User # of the person who signed on to the LPI/ELPS Terminal. If you use program keys, The Key # will also correspond to the User # of the person who made the Program keys.

```
 17) LVL 15 TYPE 2: PI CLOCK CHANGE KEY
From: LPI/ELPS  New Date:  06-08-2006 10:54AM DST

 18) LVL 15 TYPE 2: PI CLOCK CHANGE KEY
From: LPI/ELPS  Orig Date: 01-01-1980 12:02AM STD

 19) LVL 16 TYPE 0: PRIMARY PROGRAM KEY          USER #: 250
From: LPI/ELPS  Used On:   01-01-1980 12:02AM STD,  Used w/PI or Other Keys
- Capabilities: 111111111111
- CLOCK NOT SET

 20) LVL 16 TYPE 0: PRIMARY PROGRAM KEY          USER #: 250
From: LPI/ELPS  Used On:   01-01-1980 12:01AM STD,  Used w/PI or Other Keys
- Capabilities: 111111111111
- CLOCK NOT SET

 21) LVL 15 TYPE 0: SECONDARY PROGRAM KEY        USER #: 250
From: LPI/ELPS  Used On:   01-01-1980 12:01AM STD,  Programmed In by PPK
- CLOCK NOT SET

 22) LVL 16 TYPE 0: PRIMARY PROGRAM KEY          USER #: 250
From: LPI/ELPS  Used On:   01-01-1980 12:01AM STD,  Used w/PI or Other Keys
- Capabilities: 111111111111
- CLOCK NOT SET

 23) LVL 16 TYPE 3: E2 ERASE/REFORMAT KEY   PPK KEY ID#: 250     KEY #:1
From: LPI/ELPS  Used On:   06-08-2006 10:52AM DST,  Pre E2 Statuses:  PCW 000, Mode-1
                                                    Post E2 Statuses: PCW 000, Mode-2
```

LOGS INDICATING A LOCK WAS INTERROGATED OR THE LOCK'S CLOCK WAS UPDATED:

The locks clock is updated after interrogating a lock or if you select the "Update Clock" function from the terminal. The first log indicates the LPI/ELPS Program Key (only used by the LPI/ELPS Terminal) was used and then shows the two PI Clock Key logs. The first log shows the lock's original date and time and the second log shows the new date and time it was changed to. The LPI/ELPS Program key indicates the User # of the person who signed on to the terminal.

```
101) LVL 15 TYPE 2: PI CLOCK CHANGE KEY
From: LPI/ELPS  New Date:  06-08-2006 10:54AM DST

102) LVL 15 TYPE 2: PI CLOCK CHANGE KEY
From: LPI/ELPS  Orig Date: 06-08-2006 10:53AM DST

103) LVL 16 TYPE 0: LPI/ELPS PROGRAM KEY              USER #: 250
From: LPI/ELPS  Used On:   06-08-2006 10:53AM DST,  Used w/PI-DST/Clock Keys
```

8.3 UPDATING LOCKS' CLOCK DATE AND TIME

This function can be done from the transaction function 7.PROGRAM LOCKS or 8.INTERROGATE LOCKS. The transaction function 8.INTERROGATE LOCKS is easier to use. It allows you to simply update a lock's clock date and time and DST information without affecting any of the keys working in the lock.

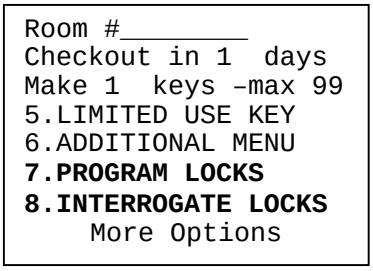
You will need an LPI/ELPS Probe to do this. If you are not allowed to update a lock, the terminal will display an error screen to indicate why. If you cannot determine what is wrong, be sure to note all the information on the screen (particularly the error #).

SPARE DESKLINC COMPUTER: If you have a Spare DeskLinc Computer Terminal, you can use it to update locks' clocks, however, you should always make sure its System Date & Time and Daylight Savings Time information is correct before using it. Refer to Section 11 for instructions on doing this.

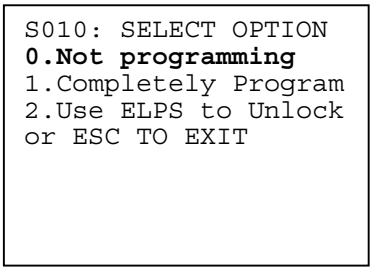
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

Step 3. Press 7 or 8 or use the ARROW DOWN key to display the 7.PROGRAM LOCK or 8.INTERROGATE LOCK menu item. Then press ENTER.



Step 4. If you chose 7.PROGRAM LOCK, the following screen (Screen 010) should appear:



Press 0, then ENTER to update locks' clock date & time.

Step 5. The following screen (Message 254) will now appear:

```
M254: Disconnect
Terminal Cables and
Connect LPI Probe
** PRESS ANY KEY **
```

Disconnect the RS232 Cable and power supply cord from the Hand-Held (also remove the printer cable if it is connected). Remove the Hand-Held Terminal from its base and connect the LPI/ELPS Probe to the printer port at the top of the terminal. Then press ANY KEY.

Step 6. One of the following menu screens (Screen 003) will now appear. You are now ready to take the terminal and ELPS?LPI probe to the lock(s).

```
S003: PROGRAM MENU 1
1.Program Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

```
S003:INTERROG MENU 1
1.Interrogate Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
```

Press 2 and ENTER to update a lock's clock date & time. Go to step 7.
Press 3 and ENTER if you are done updating locks' clocks and want to reconnect to the station and exit the transaction. Go to step 11.

Step 7. If you have the LPI/ELPS probe connected, the following screen (Message 252) will now appear. Press and key and THEN insert the LPI probe into the lock.

```
M252: Press Any Key
and THEN Insert LPI
  Probe into Lock!
(Press ESC to Abort)
```

Step 8. The terminal will then try to communicate with the lock, interrogate it and program its date & time and DST info. While it is doing this, it will beep. If the terminal detects any reason why the lock cannot be programmed, it will display an error screens (refer to Section 13.5.5). If it is able to program the lock, it will continue to beep until it is done and then display the screen in step 9.

Step 9. After the lock clock is updated, the following screen will appear. Press ANY KEY.

```
M244: LOCK xxxxx's
   CLOCK WAS UPDATED
    SUCCESSFULLY
 ** PRESS ANY KEY **
```

Step 10. The terminal will then display the following screen (Message 243).

```
M243: REMOVE PROBE
   Press Any Key to
  Program More Locks
   or ESC to Stop
```

Remove the LPI/ELPS Probe from the lock.
Press ANY KEY if you want to update more locks clocks. You will then return to step 7 for updating another lock's clock.
Press ESC if you don't want to update more locks and return to step 6.

Step 11. When you are done updating locks and select item 3.Connect to Station from the Screen 003 Program/Interrogate Menu 1, the following screen (Message 253) will appear:

```
M253: Disconnect LPI
 Probe and Reconnect
   Terminal Cables
 ** PRESS ANY KEY **
```

Disconnect the LPI/ELPS Probe from the Hand-Held. Place the Hand-Held Terminal into its Base and reconnect the RS232 Cable and power supply cord (also Printer Cable if one is normally connected). Then press ANY KEY.

The following screens will appear to indicating the Terminal is re-establishing communications with its encoder.

```
M237: PLEASE WAIT
Terminal is Signing
    Onto Station
*** ESC to Abort ***
```

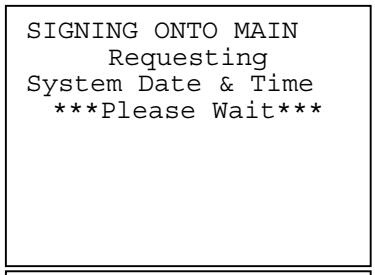
DESKLINC COMPUTER TERMINAL

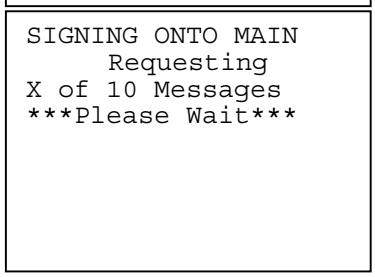
If you are using your main DeskLinc Computer Terminal and it is connected to its encoder, this will display very quickly and then proceed to Step 12.

If you are using your Spare DeskLinc Computer Terminal which does not have an encoder, you should press ESC at this screen. If you press ESC at the Message 237 screen, the Terminal will skip communications. You can then proceed to Step 12.

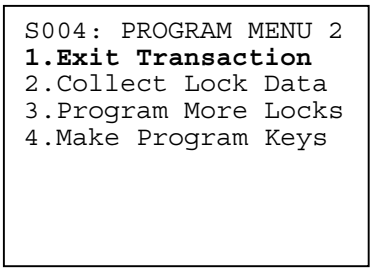
ADDITIONAL FRONT DESK TERMINAL

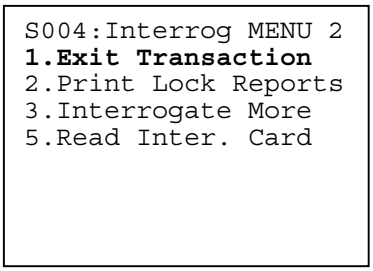
If you are using a Front Desk Terminal and it is connected to its encoder, the normal signing on messages will immediately begin displaying. If the DeskLinc Computer Terminal is on line, the 10 message collection screens will display and then proceed to Step 12.





Step 12. One of the following menu screens (Screen 004) will now appear:





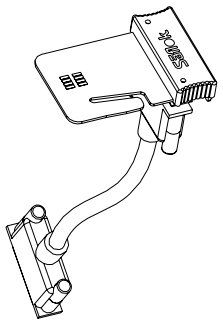
Press 1 then ENTER if you are done updating locks and want to return to the Sign On screen.

Press 3 and ENTER if you want to go update locks again. You will then return to step 5.

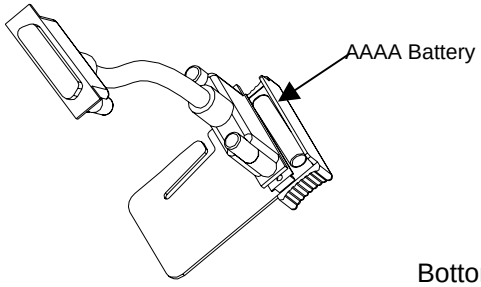
8.4 OPENING A LOCK WITH THE LPI/ELPS PROBE

The SAFLOK LPI/ELPS can be used to open a lock that has a dead internal battery. Typically a lock with a dead battery will not flash any lights after a keycard is used. If a lock displays flashing lights after a keycard is used, please refer to Section 2.3.

Lock Programmer-Interrogator/Emergency Lock Power Supply Probe



Top View

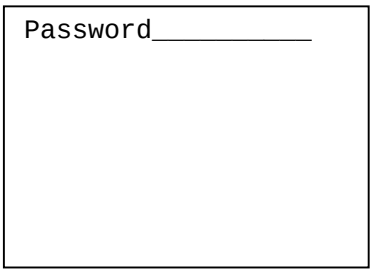


Bottom View

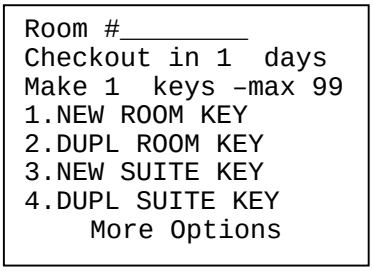
Required Equipment:

DeskLinc Handheld Computer
LPI/ELPS device with AAAA alkaline battery
Male 25DB-Male 25DB parallel cable
RS232 Cable
SAFLOK SL2500 ASIC, MT or Adese series locks (Software Version # 81305 or greater)

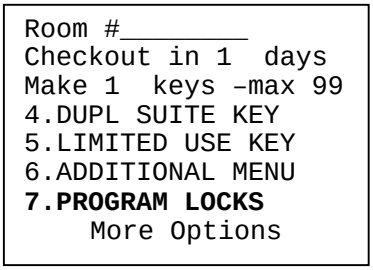
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.



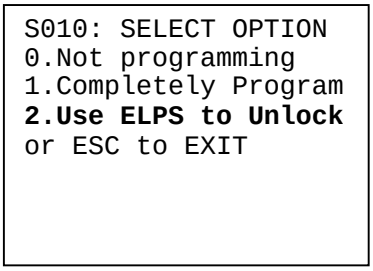
Step 2. Press ENTER three times to move the cursor to the transaction menu.



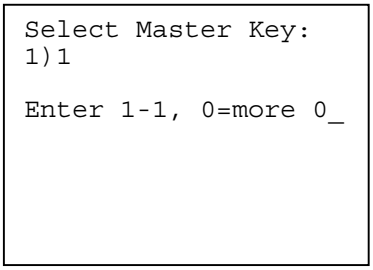
Step 3. Press 7 or use the ARROW DOWN key to display the 7.PROGRAM LOCKS menu item. Then press ENTER.



Step 4. Press 2 or use the ARROW DOWN key to display the 2. Use ELPS to Unlock menu item. Then press ENTER.



Step 5. The Seletct Master Key screen will appear. Press 1, then press ENTER.



Step 6. Disconnect the power supply cord and the RS232 cable for m the top of the hand held terminal. Connect the LPI/ELPS probe to the top of the handheld. Then press ENTER

```
M254: Disconnect
Terminal Cables and
Connect LPI Probe
** PRESS ANY KEY **
```

Step 7. Take the terminal and probe to the lock. Press 6 or use the ARROW DOWN key to display the 6. Open With ELPS Key menu item. Then press ENTER.

```
S003: PROGRAM MENU 1
1.Program Lock
2.Update Lock Clock
3.Connect to Station
4.Lock Vers/LED Diag
6.Open With ELPS Key
```

Step 8. Press any key and then insert the LPI/ELPS probe into the lock.

```
M252: Press Any Key
and THEN Insert LPI
  Probe into Lock!
(Press esc to Abort)
```

Step 9. The handheld screen will display the following message.

```
M251:  Please Wait

Programming the Lock
```

Step 10. When the handheld displays screen M236, leave the LPI/ELPS probe in the lock. Then TURN THE HANDLE.

```
M236:ELPS is powered
and the lock is open
Please turn handle
    Press Any Key
```

Step 11. After the door has been opened, remove the LPI/ELPS. Then press ESC.

```
M243: REMOVE PROBE
 Press Any Key to
Program More Locks
  or ESC to Stop
```

Press ANY KEY if you want to open more locks. You will then return to step 8 for opening another lock.

Step 12. When you are done opening a lock and select item 3.Connect to Station from the Screen 003 Program Menu 1, the following screen (Message 253) will appear:

```
M253: Disconnect LPI
Probe and Reconnect
Terminal Cables
** PRESS ANY KEY **
```

Disconnect the LPI/ELPS Probe from the Hand-Held. Place the Hand-Held Terminal in its Base and reconnect the RS232 Cable and power supply cord (and Printer Cable if one is normally connected). Then press ANY KEY.

The following screens will appear to indicating the Terminal is re-establishing communications with the encoder.

```
M237: PLEASE WAIT
Terminal is Signing
Onto Station
*** ESC to Abort ***
```

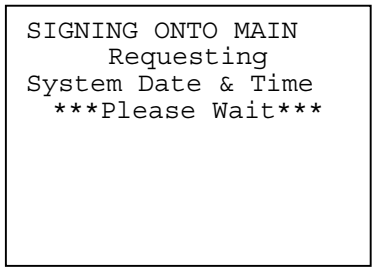
COMPUTER TERMINAL

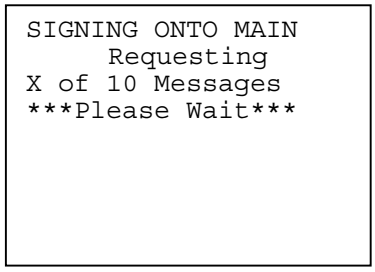
If you are using your main DeskLinc Computer Terminal and it is connected to its encoder, this will display very quickly and then proceed to Step 15.

If you are using your Spare DeskLinc Computer Terminal, which does not have an encoder, you should press ESC at this screen. If you press ESC at the Message 237 screen, the Terminal will skip communications. You can then proceed to Step 15.

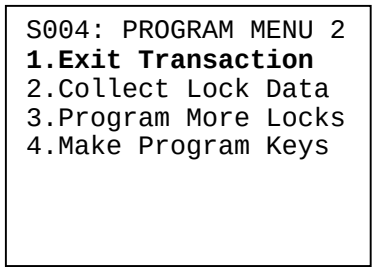
FRONT DESK TERMINAL

If you are using a Front Desk Terminal and it is connected to its encoder, the normal signing on messages will immediately begin displaying. If the DeskLinc Computer Terminal is on line, the 10 message collection screens will display and then proceed to Step 13.





Step 13. The following menu screen (Screen 004) will now appear: Press 1 for menu item 1. Exit Transaction. Then press ENTER. The handheld will return to the Password screen



******Warning***** The battery in the LPI/ELPS probe will be drained if connected to the handheld while the handheld is connected to its power supply. Please remove the LPI\ELPS device from the handheld when it is not in use**.

SECTION 9 - UPDATING USERS AND AUTHORIZATIONS

9.1 INFORMATION ON USERS & AUTHORIZATIONS

This function is used to assign, change, view or delete user names, passwords and authorizations. All individuals who will be using the terminal should be assigned user numbers passwords and authorizations.

9.1.1 User Numbers, Names, Passwords & Authorizations

User Numbers:
Each user must be assigned a unique number between 1 and 250. When adding, changing, viewing or deleting a user, you will enter this number first. Every user will have a unique user #. The user # is also logged with the transaction function information and will be printed in Tx History Reports to indicate who performed a function or made a key (see Section 10.3.2).

User Names:
The name of the user is assigned to the user number. Up to 20 characters can be entered.

Passwords:
This is a unique 3 to 10 character value that the user must enter at the password sign on screen. Although the password can be any combination of digits (0-9) and letters (A-Z), we recommend using only digits. This is because the password is not displayed when the user enters it and entering letters is more difficult (you must press the SHIFT key and press the digit key to correct number of times). You will need to give this password to the person you are adding so they can use it when signing on.

Authorizations:
There are 8 different authorization groups that can be assigned to a user. They control what functions the user will be allowed to perform. In order for the users to be able to do various functions, they must be authorized in the Main computer. Below is a list of the functions each authorization group allows.

AUTHORIZATION GROUP	FUNCTIONS AUTHORIZED
1:All Auths	All Functions
2:Front Desk	New & Duplicate Room & Suite Keys (but can't override occupied & check out errors) Miscellaneous menu functions
3:Addl FD	Overrides New & Duplicate Guest Key Errors (occupied or checked out room, etc.) Check Out a Key Limited Use Key Tx History Report Key Design Report Identify a Key
4:Failsafe Keys	New & Duplicate Failsafe Keys Miscellaneous menu functions

5:Master Keys	New & Duplicate Master Keys (Section, Floor, Grand Master, Emergency/ Security, Elect Lockout, Latch/Unlatch) Miscellaneous keys (PPK, Status, Display and SPK) Tx History Report Key Design Report Miscellaneous menu functions
6:Interrogate Lock	Interrogate Locks Update Locks' Clocks Miscellaneous menu functions
7:Program Locks	Program Locks Update Locks' Clocks Use ELPS to Unlock Miscellaneous menu functions
8:User/Key Design	Authorize Users Set System Date & DST Change System Hardware Change System Defaults Tx History Report Key Design Report User & Auth Display & Report Miscellaneous menu functions

When assigning authorizations, you should keep in mind which employees you will have available on each shift and make sure that at least one person will be authorized to perform any functions needed to take care of unexpected situations. For instance, the Front Desk will need to have someone authorized with Group 2 - Addl FD authorizations to override any new or duplicate guest key checkout or occupied room errors in order to replace a lost key or extend a guest's stay.

9.1.2 Adding a New Employee

If you need to give a new employee the ability to use the Terminals for key making, programming, interrogating, etc., you will have to assign them in the system. To determine a user # that is not currently assigned to anyone, you can view all the user #s and users in your system by following the steps in Section 10.5.1. Once you have a user #, determine which authorizations and what password you will assign them (refer to Section 9.1.1). Then follow the procedure in Section 9.3 to add the user.

9.1.3 Deleting an Employee who is Terminated

When an employee leaves your company for any reason, you should delete them from the system so they can no longer perform any functions. If you are not sure what their user # is, follow the procedures in Section 10.5.1 to view all the users in your system. Then follow procedure 9.6 to delete them.

9.1.4 Viewing an Employee's Password

If an employee forgets their password (which must be entered in order to perform any function), you can look it up for them. If you are not sure what their user # is, follow the procedures in Section 10.5.1 to view all the users in your system. Then follow the procedure in Section 9.5 to view their password and name.

9.1.5 Changing an Employee's Password, Name or Authorizations

If an employee wishes to have their password changed, changes their name or needs fewer or more authorizations, you can change the selected information. If you are not sure what their user # is, follow the procedures in Section 10.5.1 to view all the users in your system. Then follow the procedure in Section 9.4 to change the necessary information.

9.1.6 Identifying an Employee Assigned to a User

If you are reviewing a Tx History Report and wish to determine the employees assigned to various user #s, you can follow the procedure in Section 10.5.1 to view all the user #s and employees in your system.

9.2 ENTERING THE USER/AUTHORIZATION MENU

In order to do any of the functions listed in this section, you will need to first sign on and select the Additional Menu and User/Authorizations function from the Terminal's Sign On screen.

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
    More Options
```

Step 4. The following ADDITIONAL MENU screen will appear. Press 7 or use the ARROW DOWN key to display the 7.AUTHORIZE USERS menu item. Then press ENTER.

```
ADDITIONAL  MENU:
1.NEW MASTER KEYS
2.DUPL MASTER KEYS
3.CHECK OUT A KEY
4.MISCELLANEOUS KEYS
6.REPORTS
7.AUTHORIZE USERS
    More Options
```

Step 5. If you are authorized, the following menu will appear. From this menu you can select any of the functions listed in this section.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

9.3 ADDING NEW USERS

This function will allow you to add a new user to the system. Up to 30 users can be assigned passwords and authorizations.

Step 1. If you are at the Sign On screen, follow the steps in Section 9.2 to select the AUTHORIZE USERS menu. The following screen will appear.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 2. Press 1 or use the ARROW UP key to display the 1. Add New User menu item. Then press ENTER.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 3. If you have not already assigned 30 users in your system, the following screen will appear.

```
011:TO ADD A USER

Enter New User #:___
```

Enter an unused number between 1 and 250 to assign to the new user and press ENTER. If you happen to select a number already assigned to a user, you will get an error message and can select another number. If you are not sure of the available user #s, Section 10.5.1 explains how to view all the user #s and users assigned in your system.

Step 4. Once you enter a user number, the following screen will appear. The xxx in the first line will be the user number you are working on.

```
012:USER xxx INFO
Password: __________
User Name:
__________________
```

Enter a unique password between 3 and 10 characters long and press ENTER. We recommend using numbers only since the password is not displayed when the user enters it and alphabetic keys are more difficult to type. You will need to give this password to the person you are adding so they can use it when signing on.

Next, enter the name of the person you are adding (up to 20 characters) and press ENTER. Note: Remember that you can hold down the SHIFT key and press the ARROW UP key to backspace if you make a mistake.

Step 5. You will then see the following screens to assign the authorizations to the user. The xxx in the first lines will be the user number you are working on. Each authorization group will start out set at 0 - not authorized.

```
024:USER xxx AUTHS
1:All Auths ?      0
2:Front Desk ?     0
3:Addl FD ?        0
4:Failsafe Keys ?  0
5:Master Keys ?    0
6:Interrogate Lock 0
Press ENTER for more
```

```
026:USER xxx AUTHS
7:Program Locks ?  0
8:User/Key Design ?0
Press ENTER to cont.
```

For each authorization group, enter 1 to assign the authorizations or 0 not to assign. Then press ENTER. Refer to Section 9.1 for a list of the functions each authorization group allows. When you press ENTER for the last authorization group in a screen, the next screen will appear.

Step 6. After you press ENTER for the 8th authorization group, the following screen will appear.

```
M220: Do You want to
Save the Changes ?

Press 1=Yes or 0=No
```

If the user information you added was correct, press 1 to store the information. If you decide you do not want to save the information, press 0.

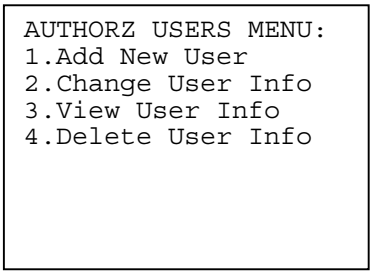
Step 7. The following screen will now appear. If you want to add, change, view or delete another user, press 1 and you will return to the AUTHORIZE USER Menu. Or press 0 to exit the transaction.

```
M221: Do You want to
Update Another User?

Press 1=Yes or 0=No
```

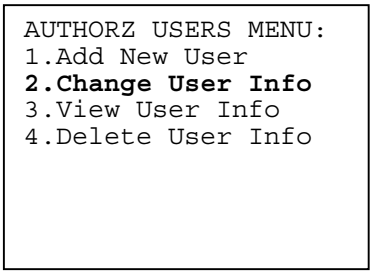
9.4 CHANGING A USER'S PASSWORD, NAME & AUTHORIZATIONS

This function will allow you to change an existing user's password, name and authorizations. **YOU SHOULD NOT REASSIGN A USER # TO A DIFFERENT PERSON USING THE CHANGE FUNCTION**. If you do, the computer will not show the correct date and time the newly assigned person was first assigned to the user #. If you wish to re-use an existing user #, first delete the existing user (Section 9.6) and then add the new user (Section 9.3).

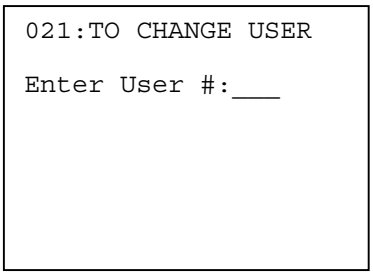
Step 1. If you are at the Sign On screen, follow the steps in Section 9.2 to select the AUTHORIZE USERS MENU. The following screen will appear.



Step 2. Press 2 or use the ARROW UP/DOWN key to display the 2. Change User Info menu item. Then press ENTER.



Step 3. The following screen will appear.



Enter the user number (between 1 and 250) of the user you want to change and press ENTER. If you happen to select a number that is not assigned to a user, you will get an error message and can select another number. If you are not sure of the user #, Section 10.5.1 explains how to view all the user #s and users assigned in your system.

Step 4. The following screen will appear showing the information for the user you selected asking if you want to change the information. Enter 1 for Yes then go to Step 5 or 0 for No then go back to Step 2.

```
022:USER 103  INFO:
Added:07-07-06 For:
SMITH-JOHN
Change? 1=Y or 0=N
```

Step 5. If you answered 1 for Yes, the following screen will appear.

```
CHANGE USER MENU:
1.Password or Name
2.Authorizations
```

If you want to change the password or name assigned to the user number, press 1 and ENTER. Then go to step 6. If you want to change the user's authorizations, press 2 and ENTER. Then go to step 7.
If you are done making changes, press ESC. Then go to Step 8.

Step 6. If you select menu item 1 from the CHANGE USER MENU, the following screen will appear. The user number you are working on will be indicated in the first line. The existing password and user name will be displayed.

```
012:USER 103 INFO
Password:
1_9_5________
User Name:
S_M_I_T_H_-_J_O_H_N
```

First you must enter the password. If you wish to keep the password the same, just press ENTER. To change it, simply enter a new unique password between 3 and 10 characters long and press ENTER. We recommend using numbers only since the password is not displayed when the user enters it and alphabetic keys are more difficult to type. You will need to give this password to the person you are adding so they can use it when signing on.

Next, you must enter the new name of the person you are changing. If you wish to keep the name the same, just press ENTER. To change it, simply enter a new unique name (up to 20 characters) and press ENTER. Note: Remember that you can hold down the SHIFT key and press the ARROW UP key to backspace if you make a mistake.

You will now return to the CHANGE USER MENU - go to Step 5.

Step 7. If you select menu item 2 from the CHANGE USER MENU, the following screens will appear. The xxx in the first lines will be the user number you are working on. The existing authorization assignments will be displayed.

```
024:USER xxx AUTHS
1:All Auths ?      0
2:Front Desk ?     1
3:Addl FD ?        1
4:Failsafe Keys ?  0
5:Master Keys ?    0
6:Interrogate Lock 0
Press ENTER for more
```

```
026:USER xxx AUTHS
7:Program Locks ?  0
8:User/Key Design ?0
Press ENTER to cont.
```

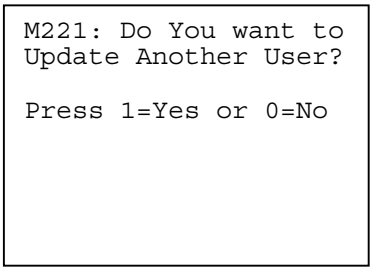
A 1 indicates the authorization group is assigned and a 0 indicates it is not. For each authorization group, you can simply press ENTER to leave it the same or enter 1 to assign the authorizations or 0 not to and then press ENTER. Refer to Section 9.1 for a list of the functions each authorization group allows.
When you press ENTER for the last authorization group in a screen, the next screen will appear.

Step 8. The following screen will appear if you actually tried to change any information. If you did not select any functions from the CHANGE USER MENU, this screen will not appear.

```
M220: Do You want to
Save the Changes ?

Press 1=Yes or 0=No
```

If the user information you changed was correct, press 1 to store the information. If you decide you do not want to save the changes, press 0.

Step 9. The following screen will now appear. If you want to add, change, view or delete another user, press 1 and you will return to the AUTHORIZE USER MENU where you can select another menu item or press 0 to exit the transaction.



9.5 VIEWING A USER'S PASSWORD AND NAME

This function will allow you to view the password and name assigned to a user number and the date they were added. This function will not let you view the authorizations. You must choose the 2.Change User Info function if you want to see the authorization groups assigned.

Step 1. If you are at the Sign On screen, follow the steps in Section 9.2 to select the AUTHORIZE USERS MENU. The following screen will appear.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 2. Press 3 or use the ARROW UP/DOWN key to display the 3. View User Info menu item. Then press ENTER.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 3. The following screen will appear.

```
031:TO VIEW USER

Enter User #:___
```

Enter the user number (between 1 and 250) of the user you want to view and press ENTER. If you happen to select a number that is not assigned to a user, you will get an error message and can select another number. If you are not sure of the user #, Section 10.5.1 explains how to view all the user #s and users assigned in your system.

Step 4. Once you enter a user number, the following screen will appear. The user number you are viewing is indicated in the first line. The existing password, date the user was added and existing user name will also be displayed.

```
032: USER 103 INFO:
Password: 195
Added: 06/15/06 For:
SMITH-JOHN
```

When you are done viewing the information, press any key or ESC.

Step 5. The following screen will now appear. If you want to add, change, view or delete another user, press 1 for Yes and you will return to the AUTHORIZE USER MENU. Or press 0 for No and return to the Password/Sign On screen.

```
M221: Do You want to
Update Another User?

Press 1=Yes or 0=No
```

9.6 DELETING A USER

This function will allow you to delete a user including the password, name and authorizations assigned.

Step 1. If you are at the Sign On screen, follow the steps in Section 9.2 to select the AUTHORIZE USERS MENU. The following screen will appear.

```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 2. Press 4 or use the ARROW UP/DOWN key to display the 4. Delete User Info menu item. Then press ENTER.

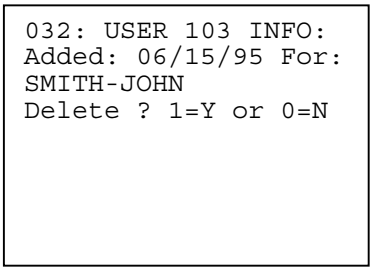
```
AUTHORZ USERS MENU:
1.Add New User
2.Change User Info
3.View User Info
4.Delete User Info
```

Step 3. The following screen will appear.

```
041:TO DELETE USER

Enter User #:___
```

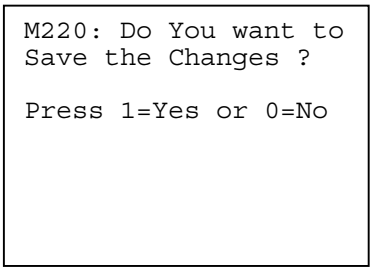
Enter the user number (between 1 and 250) of the user you want to delete and press ENTER. If you happen to select a number that is not assigned to a user, you will get an error message and can select another number. If you are not sure of the user #, Section 10.5.1 explains how to view all the user #s and users assigned in your system.

Step 4. Once you enter a user number, the following screen will appear. The user number you are deleting is indicated on the first line. The date the user was added and the user name currently assigned will also be displayed.



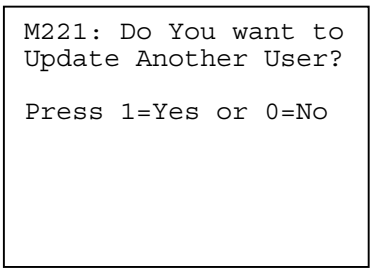
If you want to continue and delete the user, press 1 for Yes. Then go to Step 5. If you decide not to delete the user, press 0 for No and go to Step 6.

Step 5. If you entered 1 to delete the user, the following screen will appear. If you entered 0, not to delete the user, this screen will return to the AUTHORIZE USERS MENU.



If you want to save the changes and delete the user, press 1 for Yes. If you decide you do not want to delete the user, press 0 for No.

Step 6. The following screen will now appear. If you want to add, change, view or delete another user, press 1 and you will return to the AUTHORIZE USER MENU. You can then begin at step 1 in the section for the function you want to do. Press 0 for No to return to the Password screen.



SECTION 10 - REPORTS

10.1 INFORMATION ON REPORTS

This function is used to print a variety of reports. The reports can only be requested at the DeskLinc Main Terminal. You will not be able to use the DeskLinc Main Terminal for any other functions until the report is finished. The various reports covered in this section include the TX History, Key Design and User & Authorizations. Another report, the Lock Interrogation Report, is explained in Section 8.2.

TX HISTORY REPORT This report prints the history of transactions or functions that are performed at the computer system. It includes all key making and other functions. The report is typically used for the following purposes:
- to determine if a key stopped working because someone made a New key
- to verify when keys were made and who made them
- to verify that employees are using cleaning keys to clean the encoders
- to troubleshoot various system equipment problems

KEY DESIGN REPORTS These reports print the information on your property's Key Design. There are three reports which include all the default settings, all the locks and key mastering and all the keys with a listing of the locks they work in. The reports are typically used for the following purposes:
- to check your default settings
- to verify what keys should work in a lock
- to verify what lock's a key should work in
- to determine the Key #s to use when making Suite, Master, PPK & SPK keys

There are three different reports you can select. Report 1 includes settings that can be changed using the 9.SYSTEM DESIGN function as well as your system Daylight Savings Time settings and how many locks or keys are currently in your design. Report 2 allows you to print out all your locks with all the different keys that should work in each one. Report 3 allows you to print out all the different keys in your system with all the locks each key should work in.

USER & AUTHORIZATIONS REPORT This function will allow you to view a user's information, view all the users in your system or print all your users' information and the authorization group functions. The reports print the current users and authorizations that are assigned in the computer system. This function is typically used for the following purposes:
- to view all the user #s assigned in your system
- to verify that all your users and authorizations are up-to-date
- to identify who is assigned to a user # that prints in the Tx History Report or a Lock Interrogation Report
- to identify unused user #s you can use to assign to new users
- to review what terminal functions are associated with each authorization group

There are two different reports that will print. Report 1 prints the users assigned in your system, including the user #, name, authorizations, date they were added and last date they were changed. It will not print passwords. Report 2 prints a listing of all the functions that each authorization group will allow a user to select.

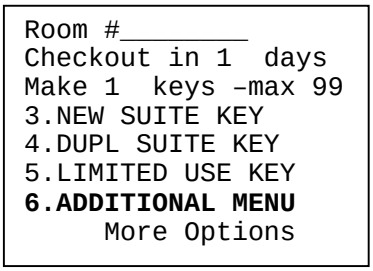
10.2 ENTERING THE REPORTS MENU

In order to do any of the reports listed in this section, you will need to first sign on and select the 6.ADDITIONAL MENU and the 6.REPORTS function from the Terminal's Sign On screen.

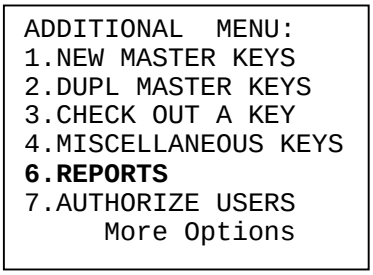
Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

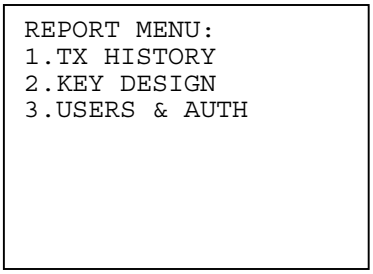
Step 3. Press 6 or use the ARROW DOWN key to display the 6.ADDITIONAL MENU item. Then press ENTER.



Step 4. The following ADDITIONAL MENU screen will appear. Press 6 or use the ARROW DOWN key to display the 6.REPORTS menu item. Then press ENTER.



Step 5. The following menu will appear. From this menu you can select any of the report functions listed in this section.

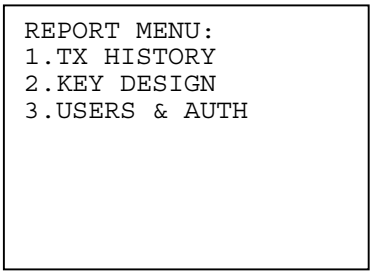


10.3 TX HISTORY REPORT

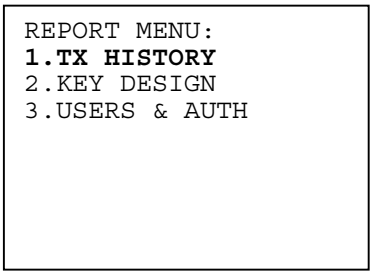
10.3.1 Requesting the TX History Report

This report will allow you to selectively print a history of the transaction functions that have been performed on the computer system. It can only be requested at the DeskLinc Main Terminal and will require the System Printer to be connected and available. You will not be able to use the DeskLinc Main Terminal for any other functions until the report is finished.

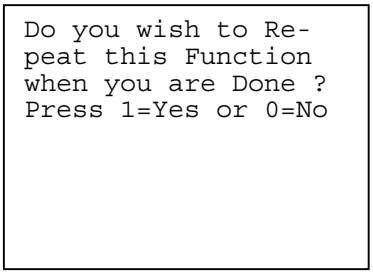
Step 1. If you are at the Sign On screen, follow the steps in Section 10.2 to select the REPORTS MENU. The following screen will appear.



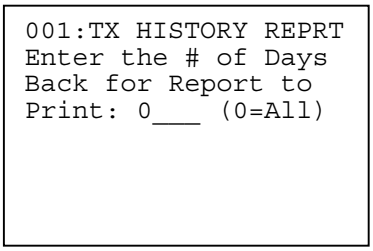
Step 2. Press 1 or use the ARROW UP key to display the 1.TX HISTORY menu item. Then press ENTER. If you are done printing reports, press ESC to return to the Sign On screen.



Step 3. If you want to do several Tx History or other reports, we suggest you press 1 for Yes. If you do, you will return to the REPORT MENU screen after you are done with a report instead of returning all the way back to the Sign On screen.



Step 4. If you have authorization 1.ALL Auths, 3.Addl FD, 5.Master Keys or 8.User/Key Design, the following screen will now appear. You will now specify the # of days back the report should begin. If you wish to print transactions as far back as possible, enter 0 and press ENTER. If you only wish to print transactions since a certain date, enter the # of days back the report should start and press ENTER.

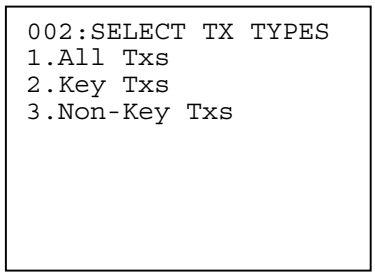


Step 5. You will now be asked if you want to specify the types of transactions that should be printed.
Key Txs include only transactions which make or affect keys - new, duplicate or check out guest keys, new or duplicate failsafe & master keys and special keys. Non-Key Txs include all the other functions you can do on the system. All Txs, of course, include both Key & Non-Key transaction functions.

If you are trying to trouble shoot a lock's keycard or other problem, we would suggest selecting 1. You will then see the screen shown in Step 6

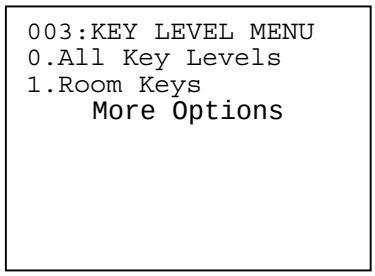
If you are only interested in reviewing the keys you have made (such as for Room, Failsafe or Master keys), you can select 2. You will then see the screen shown in Step 6

If you are only interested in reviewing recent changes to your users or authorizations, or want to know if reports were printed, Key Design changes were made, etc., you can select 3. You will then see the screen shown in Step 8



Press the number of the selection you want or use the ARROW keys to position the cursor and press ENTER.

Step 6. You will now be asked if you want to specify a specific Key Level to print. If, for instance you are only interested in a report on Failsafe keys you recently made, pre-made Room keys or a particular Guest or Master key you have a problem with, you can select the specific key level you want. If you want a report of keys for more than one level, you must select 0.All Key Levels or do individual reports for each key level.



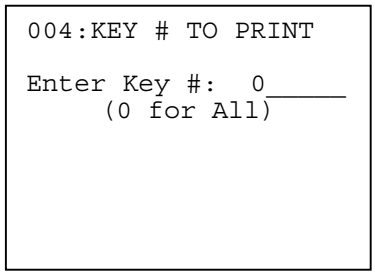
Key Level Menu Selections
0. All Key Levels
1. Room Keys
2. Suite Keys
3. Limited Use Keys
4. Failsafe Keys
5. Section Keys
6. Floor Keys
7. Latch/Unltch Keys
8. Inhibit Keys
9. Grand Master Keys
A. Securty/Emerg Keys
B. Elect Lockout Keys
C. SPK Keys
D. PPK Keys

Press the number of the selection you want or use the ARROW keys to position the cursor and press ENTER.

Step 7. You will now be asked if you want to specify that only transactions related to a specific key # be printed. You would usually only select a specific key # if you were investigating a problem with a specific key.

If you are only interested in reviewing a specific key, you can enter the key # and press ENTER. For Room and Failsafe keys, you would enter the room #, but for all other keys, you must enter the Suite or Master key #. The Key Design Report #3 can provide you with the Key #s for all your keys (refer to Section 10.4 for this report).

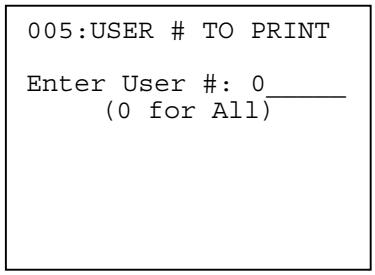
If you are not investigating a specific key, enter 0 and press ENTER.



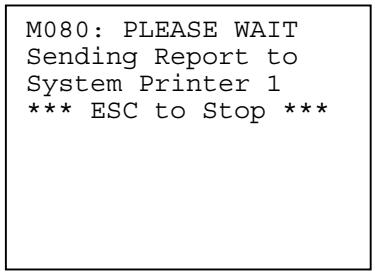
Step 8. You will finally be asked if you want to specify that only transactions performed by a particular user (employee) be printed. You would usually only select a specific user # if you were only re-checking whether someone made keys for the wrong room or master area.

If you are interested in only reviewing a specific user's transactions, you can enter their user # and press ENTER. You do NOT enter their password; you must enter the user # they were assigned (see Section 10.5 to view or print the users in your system if necessary).

If you are not investigating a specific user's transactions, enter 0 and press ENTER.



Step 9. Assuming your printer is connected to the Terminal and is not being used by another station, the terminal will display the following screen and will begin printing the report. You cannot use the terminal again until the report is done. If you have an emergency, you can press ESC to abort the report.



Step 10. When the report is done, or if you press ESC or time out at any point after step 3, the transaction will end.

If you indicated 1=Yes in Step 3, you will now return to the REPORTS MENU screen (Step 5) and can select another report.

If you indicated 0=No in Step 3, you will now return to the Password/Sign On screen.

10.3.2 Reading the TX History Report

Transaction History Report - Sample Report

Below is a sample of the Transaction History Report. Explanations of how to read it are provided on the following pages.

PAGE 1 06-30-2006 11:22AM DST DESKLINC SYSTEM TERMINAL # 1

TX HISTORY REPORT: 06-01-2006 09:00AM to 06-01-2006 11:59PM (MM-DD-YY)

REPORT INCLUDES ALL TXS WITHIN THE DATE RANGE

TX DESCR	KEY #	# OF KEYS	LAST ID# /TO USER	BY USER	BY STA#	FROM STA#	TX STATUS INFO S-ERROR-ACTION	TX STARTED DATE & TIME
New Room	#101	1	1	14	2	2	C-190-0	06-01-06 19:16
New Room	#214	1	1	14	2	2	C-190-0	06-01-06 19:18
New Room	#121	1	1	17	1	1	C-189-0	06-01-06 19:21
Dupl Floor	#1	1	7	22	1	1	C-189-0	06-01-06 19:22
New Room	#146	1	1	17	1	1	C-189-0	06-01-06 19:47
New Room	#187	2	2	14	2	2	C-190-0	06-01-06 19:50
Interrogate		0	0	22	1	2	C-0 -0	06-01-06 19:52
Dupl Room	#214	1	2	14	1	1	C-189-0	06-01-06 20:16
New Room	#205	1	1	17	1	1	C-189-0	06-01-06 21:23
New Room	#161	1	1	17	1	1	C-189-0	06-01-06 21:26
New Room	#227	1	1	14	2	2	C-189-0	06-01-06 21:29
New Room	#100	1	1	14	2	2	C-189-0	06-01-06 21:31
New Room	#114	2	2	17	1	1	C-190-0	06-01-06 21:32
New Room	#225	1	1	14	2	2	C-189-0	06-01-06 21:34
New Suite	#214	1	1	17	1	1	C-190-0	06-01-06 21:45
Dupl Room	#173	1	2	14	2	2	C-190-0	06-01-06 21:49
New Room	#244	1	1	14	2	2	C-189-0	06-01-06 21:50
New Room	#178	0	1	14	1	2	A-190-0	06-01-06 21:55
New Room	#178	1	1	14	2	2	C-189-0	06-01-06 22:05
New Room	#209	1	1	14	2	2	C-189-0	06-01-06 22:27
New Room	#235	1	1	14	2	2	C-189-0	06-01-06 23:23
New Room	#230	1	1	12	1	1	C-190-0	06-02-06 08:32
New Room	#121	1	1	12	1	1	C-189-0	06-02-06 09:00
Auth Users		2	10	25	1	1	C-0 -1	06-02-06 09:09
New Room	#146	1	1	10	2	2	C-189-0	06-02-06 09:52
New Room	#244	1	1	12	1	1	C-189-0	06-02-06 10:39
Dupl Room	#178	1	2	12	1	1	C-190-0	06-02-06 10:42
New Room	#207	1	1	10	2	2	C-190-0	06-02-06 11:25
New Room	#197	1	1	12	1	1	C-189-0	06-02-06 11:43
New Room	#130	1	1	10	2	2	C-189-0	06-02-06 12:28

Transaction History Report - Information Explanation

At the top of the report, the range of dates used for the report are printed. If you also specified that you only wanted to print transactions meeting certain criteria (key related, key level, key # or user #), the report indicates that only these transactions will be printed.

The remainder of the report lists the transactions which met the criteria you specified. Each transaction prints the following information:

TX DESCRIPTION - This identifies the transaction function that was selected.

KEY # - If the transaction was related to a particular key, the key # is printed. For room keys, this is the same as the room #.

 # OF KEYS - If the transaction was related to making keys (New, Duplicate & Special keys), the number of keys that were made is indicated. 0 indicates that no keys were actually made.

LAST ID#/TO USER - If the transaction was related to a particular key, the last key ID# made for the key is printed. If the # of Keys column shows 0 keys, it is simply the last ID# previously made.

If the transaction is "Auth Users", this column represents the user # that was added, changed, viewed or deleted.

BY USER - This is the User # of the person who performed the transaction. To determine the name of the person who has this user #, refer to Section 10.5 Users & Authorizations Report.

BY STA# - This is typically the Encoder or terminal that actually encoded the key or performed the transaction activity. For key making transactions, it is the encoder that made the key. If keys were not made, it is will probably be set to station 1 - the DeskLinc Computer Terminal.

FROM STA# - This is the Terminal or PMS Interface station that actually requested the transaction. For keys made through a PMS Interface station, it will be the PMS Interface station # and the BY STATION column would show the encoder the key was made at. Requests that are done at Additional Front Desk Terminals, this will be the Terminal station # and the BY STATION column would show the same station # of the encoder the key was made at.

TX STATUS INFO : S-ERROR-ACTION - This transaction status info consists of three pieces of information separated by dashes.

S (Status)

- C = Transaction was Completed

  In key making transactions, this indicates that keys were actually made. In other transactions it indicates that the transaction was successfully entered, but no changes were necessarily made. Transactions such as reports and design changes may log as complete even though nothing was actually changed or printed. In these cases, the ACTION code indicates if anything was actually changed.

- A = Transaction was Aborted

  In key making transactions, this indicates that no keys were actually made. For most other transactions, it indicates that nothing was actually done or nothing was changed. The ERROR code that follows typically corresponds to a general error or a transaction error which explains why it was aborted.

- I = Transaction was Incomplete

  This typically appears for the Tx History transaction and indicates that the transaction has not been ended yet. If it appears for other transactions, it normally indicates the encoder or terminal power was reset in the middle of doing a transaction, so the computer did not know the final status of the transaction.

ERROR

Whether a transaction was completed or not, it often will log an error code. The error code indicates either why the transaction was aborted or indicates an error the user decided to override in order to complete the transaction. Section 13.5 contains explanations for the error codes that may be logged. They are the same codes as the error screens which display on the terminal. Error codes 189 (user pressed ESC) and 190 (transaction timed out) are the most common and indicate normal ways to exit a transaction.

ACTION

Transactions where different actions can be taken will also include an action code to indicate what was done. For instance, when the Auth Users transaction is completed, the user that was affected could have been added, viewed, changed or deleted. The action code indicates which of these things was done. Each transaction has different action codes. Explanations for the codes are provided on the following pages.

TX STARTED DATE & TIME This indicates the date and time the transaction was started. When a transaction is requested, the system date & time is logged. The transactions are logged and printed out in chronological order. If, however, the System Date & Time in the DeskLinc Terminal has been changed, the transactions may not print out in chronological order.

Transaction History Report - Transaction ACTION Code Explanations

The following transactions may log an action code when they are performed. In some cases, the code must be converted to a binary number (eight 0's or 1's) to determine what it means. This is indicated where applicable.

New Key: The action code for this function is bit specific - the decimal # must first be converted to binary and each of the 8 bits mean something different:

Bit 0 - If this bit = 1, the Action code will = 1 or 129.
Error 203 occurred indicating that the user should have replaced any previously made keys with new keys since the computer had no record of any previously made keys.

Bit 7 - If this bit = 1, the Action code will = 128 or 129.
Error 229 or 228 occurred indicating that the computer noticed that the new key date of the last new key was greater than the system date & time when the new key was requested. This indicates that at an earlier point, the system date & time was incorrectly set to a future date and/or time.

Dupl Key: The action code for this function is bit specific - the decimal # must first be converted to binary and each of the 8 bits mean something different:

Bit 0 - If this bit = 1, the Action code will = 1, 3, 5, 7, 129, 131, 133 or 135.
Error 200, 203 or 204 occurred indicating that the user should have replaced any previously made keys with new keys since the computer had no record of any previously made keys.

Bit 1 - If this bit = 1, the Action code will = 2, 3, 6, 7, 130, 131, 134 or 135.
It should only occur for non-guest keys and indicates that the user was re-making key IDs instead of making additional duplicate keys.

Bit 2 - If this bit = 1, the Action code will = 4, 5, 6, 7, 132, 133, 134 or 135.
Error 212 or 213 occurred and the key was previously checked out by someone. It also indicates that the key was checked back in when the duplicate key was made.

Bit 7 - If this bit = 1, the Action code will be between 128 and 135.
Error 229 or 228 occurred indicating that the computer noticed that the new key date of the last new key was greater than the system date & time when the new key was requested. This indicates that at an earlier point, the system date & time was incorrectly set to a future date and/or time.

Chkot Key: There are no action codes for this function.

PPK Key: There are no action codes for this function.

SPK Key: There are no action codes for this function.

Status Key: The Action code indicates the type of status key made:
1 = LED Diagnostic key
3 = E2 Erase key

Display Key: The Action code indicates the type of display key made:
1 = E2 Program Version 2 = Lock Clock Time 3 = Lock Clock Date 4=Interrogation
6 = Knob Switch Status 7 = Dead Bolt Status 9 = Low Battery Status

Program Lock: There are no action codes for this function.

Interrogate: There are no action codes for this function.

Design Reprt: Action code = 1 indicates a report was actually printed.

User Report: There are no action codes for this function.

Tx History: Action code = 1 indicates a report was actually printed.

Set DateTime: The action code for this function is bit specific - the decimal # must first be converted to binary and each of the 8 bits mean something different:
Bit 0 - If this bit = 1, the Action code will = 1, 5, 17, 21, 33 or 37.
It indicates that the new time was changed from DST time to standard time.
Bit 1 - If this bit = 1, the Action code will = 2, 6, 18, 22, 34 or 38.
It indicates that the new time was changed from standard time to DST time.
Bit 2- If this bit = 1, the Action code will = 4, 5, 6, 20, 21, 22, 36, 37 or 38.
It indicates that the system date or time was actually changed.
Bit 4- If this bit = 1, the Action code will be between 16 and 22.
It indicates that the new date entered was 1 or more days prior to the original system date.
Bit 5- If this bit = 1, the Action code will be between 32 and 38.
It indicates that the new date entered was 7 or more days later that the original system date.

Set DST Info: The action code for this function is bit specific - the decimal # must first be converted to binary and each of the 8 bits mean something different:
Bit 0 - If this bit = 1, the Action code will = 1, 3, 129, or 131.
It indicates that the DST start & end dates or times were changed, but not the DST Option.
Bit 1 - If this bit = 1, the Action code will = 2, 3, 130, or 131.
It indicates the user changed the DST Option in the system.
Bit 7 - If this bit = 1, the Action code will be between 128 and 135.
It indicates that the new DST info caused the computer to change the system time from standard to DST time or vice versa.

Terminal Set: There are no action codes for this function.

Hrdwr Desgn: There are no action codes for this function.

Deflt Desgn: Action code = 1 indicates that some information may have been changed.

Auth Users: The Action code indicates what was done to the user indicated in the "TO USER" column:
1 = user was added 2 = user was changed 3 = user was viewed 4 = user was deleted

Commun Chng: There are no action codes for this function.

Status Log: The Action code indicates what change in station status occurred.
9 = Load Program: The terminal's program was restarted from the Power Up Menu screen.
11= Main Computer Logged onto System: The terminal was a Main and re-started communications.
14= Slave Signed onto Main: The terminal was a slave & re-signed on to the Main.
26= Station Hardware Reset: The encoder station's power was reset.
27= Station Software Reset: The encoder or station reset due to a software time out.

Printer/Test: There are no action codes for this function.

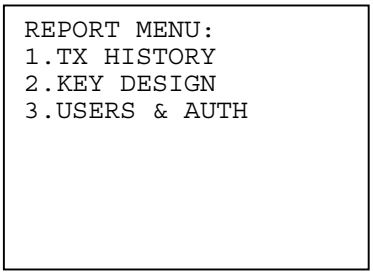
Exit Program: Action code = 1 indicates that the Terminal's program was actually exited to the Power Up Menu.

10.4 KEY DESIGN REPORT

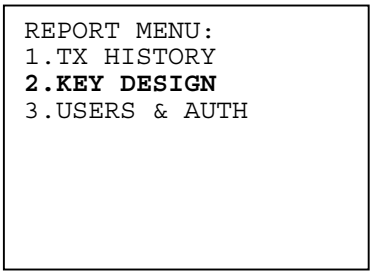
10.4.1 Requesting the Key Design Report

This report will allow you to print information on your Key Design. There are three different reports you can select. Report 1 includes settings that can be changed using the 9.SYSTEM DESIGN function as well as your system Daylight Savings Time settings and how many locks or keys are currently in your design. Report 2 allows you to print out all your locks with all the different keys that should work in each one. Report 3 allows you to print out all the different keys in your system with all the locks each key should work in.
This function can only be requested at the DeskLinc Main Terminal and will require the System Printer to be connected and available. You will not be able to use the DeskLinc Main Terminal for any other functions until the report is finished.

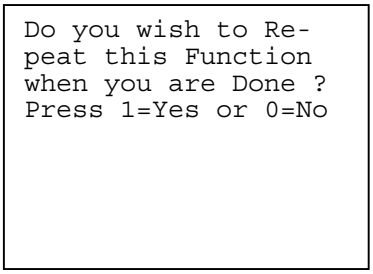
Step 1. If you are at the Sign On screen, follow the steps in Section 10.2 to select the REPORTS MENU. The following screen will appear.



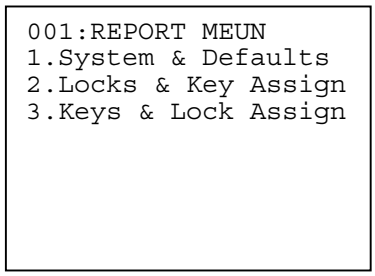
Step 2. Press 2 or use the ARROW DOWN key to select the 2.KEY DESIGN menu item. Then press ENTER. If you are done printing reports, press ESC to return to the Sign On screen.



Step 3. The following screen will now appear. If you want to do several Key Design or other reports, we suggest you press 1. If you do, you will return to the REPORT MENU screen after you are done with a report instead of returning all the way back to the Sign On screen.



Step 4. If you have authorization 1.ALL Auths, 3.Addl FD, 5.Master Keys or 8.User/Key Design, the following screen will appear.



If you want to print Report 1, press 1 or use the ARROW keys to select 1.System & Defaults. Then press ENTER. The computer will then try to print the report (go to step 12).

If you want to print Report 2, press 2 or use the ARROW keys to select 2.Locks & Key Assign. Then press ENTER. Then go to step 5.

If you want to print Report 3, press 3 or use the ARROW keys to select 3.Keys & Lock Assign. Then press ENTER. Then go to step 8.

If you do not want to print any more reports, press ESC to return to the Password/Sign On screen or the main Reports Menu:

- If you indicated 1=Yes in Step 3, you will now return to the REPORTS MENU screen (Section 10.2 , Step 5) and can select another report.

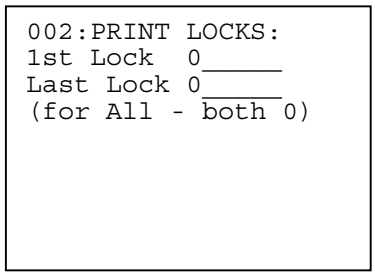
- If you indicated 0=No in Step 3, you will now return to the Password/Sign On screen.

Step 5. If you selected report 2 in step 4, the following screen will appear. You are now asked if you want to print all the locks or to specify a range of locks.

If you want to print all the locks, simply press ENTER twice, leaving both lock values 0.

If you want to print one lock, enter the lock or room # for the 1st lock and press ENTER. You can leave the last lock 0 and press ENTER again.

If you want to print a range of locks, enter the lower room # for the first lock and press ENTER. Then enter the higher room # for the last lock and press ENTER.



Step 6. You will now be asked if you will want to print more locks after the computer prints the lock range you specified in step 5. If you will want to return to step 5 and enter another range after the report prints, press 1. Otherwise, press 0 so you will return to step 4 after the report prints.

```
Do You want to Print
More Locks After the
Report Prints ?
Press 1=Yes or 0=No
```

Step 7. The following screen will next appear indicating the computer is sorting the locks to print them in numerical and alphabetic order. When this is done, the computer will then try to print the report (go to step 12).

```
   Selecting and
   Sorting Lock
   or Key names
** PLEASE WAIT **
```

Step 8. If you selected report 3 in step 4, the following screen will appear. You will now be asked to specify a specific Key Level to print. If, for instance you are only interested in a report of all your Failsafe keys or you are only interested in the locks a particular Master key works in, you can select the specific key level you want. If you want a report of keys for more than one level, you must select 0.All Key Levels or do individual reports for each key level.

```
003:KEY LEVEL MENU
0.All Key Levels
1.Room Keys
2.Suite Keys
    More Options
```

Key Level Menu Selections
0.All Key Levels
1.Room Keys
2.Suite Keys
3 Limited Use Keys
4.Failsafe Keys
5.Section Keys
6.Floor Keys
7.Latch/Unltch Keys
8.Inhibit Keys
9.Grand Master Keys
A.Securty/Emerg Keys
B.Elect Lockout Keys
C.SPK Keys
D.PPK Keys

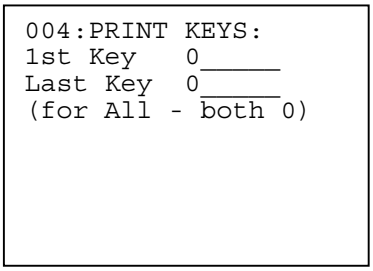
Press the number of the selection or use the ARROW keys to position the cursor and press ENTER.

Step 9. You are now asked if you want to print all the keys or to specify a range of keys.

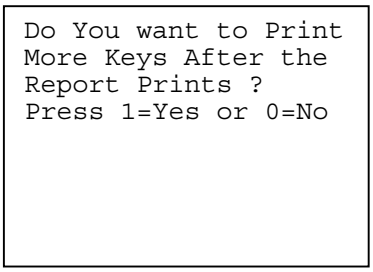
If you want to print all the keys, simply press ENTER twice, leaving both key values 0.

If you want to print one key, enter the key # for the 1st key and press ENTER. You can leave the last key 0 and press ENTER again.

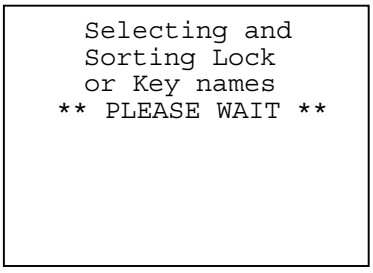
If you want to print a range of keys, enter the lower key # for the first key and press ENTER. Then enter the higher key # for the last key and press ENTER.



Step 10. You will now be asked if you will want to print more keys after the computer prints the key range you specified in step 9. If you will want to return to step 9 and enter another range after the report prints, press 1. If you want to select a different key level, you should press 0 so you will return to step 4 instead.



Step 11. The following screen will next appear indicating the computer is sorting the keys to print them in numerical and alphabetic order. When this is done, the computer will then try to print the report (go to step 12).



Step 12. Assuming your printer is connected to the Terminal and is not being used by another station, the terminal will display the following screen and will begin printing the report. You cannot use the terminal again until the report is done. If you have an emergency, you can press ESC to abort the report.

```
M080: PLEASE WAIT
  Sending Report to
  System Printer 1
 *** ESC to Stop ***
```

Step 13. When the report is done, or if you press ESC or time out at any point after step 3, the transaction will return to let you select another report or it will end.

If you were printing Report 1, you will now return to the Step 4 Key Design REPORTS MENU screen and can select another key design report.

If you were printing Report 2 and you indicated 1=Yes in Step 6, you will now return to Step 5 so you can enter another lock range. If you indicated 0=No in Step 6, you will now return to the Step 4 Key Design REPORTS MENU screen and can select another key design report.

If you were printing Report 3 and you indicated 1=Yes in Step 10, you will now return to Step 9 so you can enter another key range. If you indicated 0=No in Step 10, you will now return to the Step 4 Key Design REPORTS MENU screen and can select another key design report.

When finished printing reports, press ESC to return to the Password/Sign On screen.

10.4.2 Reading the Key Design Report

Key Design Report 1 - Sample Report - Page 1

Below is a sample of the first page of the System & Defaults Report. Explanations of how to read it are provided on the following pages.

```
PAGE 1     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

LOCK & KEY DATA FILE DESIGN INFORMATION:  REPORT # 1
--------------------------------------------------------------------------------
Using PROPPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 1-42
Using PROPSYS.ACT Vers: 06-14-2006  Prop#: 100   Seq: 11-7
Using NAMEINDX.ACT Vers: 06-14-2006  Prop#: 100   Seq: 7-0
Using KEYPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 2-7
SYSTEM INFO & DEFAULT SETTINGS:

"Default" indicates a field value that is displayed in screens when making keys
          and can be changed if desired

GENERAL SYSTEM PARAMETERS:
Property #     100
Property Type  1
Date Format    MM-DD-YYYY
Locks will never force you to reprogram their clock Date & Time
Daylight Savings Time Changes occur every year as follows:
  DST STARTS 1st Sun of Apr at 02:00AM & ENDS last Sun of Oct at 02:00AM
Additional Key Data is Encoded on NO Keys.
Password Sign On Times Out after every Tx.

SYSTEM HARDWARE AND SIZING:
Station #
    2    Max # of Stations in the System
    1    System Printer


DATA FILE SIZING:
Locks:    Max # 318      Current # 145
Keys :    Level   Max #  Current #      Level   Max #  Current #
          Room    318      106          Suite   158      21
          Failsf  318      106          Section 30       15
          Lim Use 318      106
          Floor   30       2            Latch   30       2
          Inhibit 30       2            G Mastr 30       2
          Emerg   30       2            Lockout 30       2
          SPK     62       1            PPK     62       1

32   Max # Authorized User Assignments Allowed
```

Key Design Report 1 - Sample Report - Page 2

Below is a sample of the second page of the System & Defaults Report. Explanations of how to read it are provided on the following pages.

```
PAGE 2     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

LOCK & KEY DATA FILE DESIGN INFORMATION:  REPORT # 1
--------------------------------------------------------------------------------
Using PROPPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 1-42
Using PROPSYS.ACT Vers: 06-14-2006  Prop#: 100   Seq: 11-7
Using NAMEINDX.ACT Vers: 06-14-2006  Prop#: 100   Seq: 7-0
Using KEYPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 2-7
SYSTEM INFO & DEFAULT SETTINGS:

"Default" indicates a field value that is displayed in screens when making keys
          and can be changed if desired

FOR KEYS DESIGNATED AS FAILSAFE KEYS:
3 Sequences of New Failsafe keys must be Pre-Made & Stored

FOR GUEST KEYS WITH CHECKOUT DATES:
  2     Default Checkout Date = # of days from the date a New key is made
12:00pm Checkout Time
  31    Max Checkout Date Warning = # days from the default checkout date
        checkout date can be without causing a warning
A Key is Assumed to be Checked Out once its Checkout Date Passes.
Guest keys Do NOT Override Dead Bolts.

NEW KEY WARNING MESSAGES:
New Key Warning Group & # of days from the date a New key is made to display a
warning if another new key is attempted (0=no warning).
  0  days for Failsafe
  31 days for Section, Floor, Latch, Inhibit
  62 days for Grand Master, Emergency & Lockout
  62 days for PPK & SPK

KEY EXPIRATION DEFAULTS:
- Guest Keys w/Checkout       7    0    = # days, hrs from Checkout Date & Time
- Failsafe Keys               7         = # days from date New key is Used
- Sectn,Floor,Ltch,Inhbt Keys 31        = # days from date New key is Made
- GMastr,Emerg,Lockout Keys   365       = # days from date New key is Made
- SPK Keys                    1         = # days from date New key is Made
- PPK Keys                    511       = # days from date New key is Made
```

Key Design Report 1 - Information Explanation

Report 1 includes settings that can be changed using the 9.SYSTEM DESIGN function as well as your system Daylight Savings Time settings and how many locks or keys are currently in your design. This report consists of two pages.

GENERAL SYSTEM PARAMETERS - This section contains some fixed system settings, some settings that can be changed using function 9.SYSTEM DESIGN and the DST settings which can be set using function 8.SYSTEM DATE & DST.

Property # - This is your property's pre-assigned, unique property #.

Property Type - This is set to 1 to indicate you have a DeskLinc System.

Date Format - This is set to MMDDYY or DDMMYY depending on what Date Format was selected in the 9.SYSTEM SETTINGS - 2.SYSTEM DEFAULTS function. Dates on the terminal screens and printouts will indicate either the month then date or the date then month based on this setting.

Lock Clock Reprogramming - This line indicates whether your locks will require you to reprogram their clocks every 1 to 15 months or never. If a # of months is indicated, each lock will display a red light with their normal lights when keys are used if the lock has not had its clock updated in the # of months indicated. It can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

Daylight Savings Time - This information indicates whether your system uses DST and if so, when DST starts and ends for the current year. It can be changed using the 8.SYSTEM DATE & DST - 2.DST SETTINGS function.

Additional Key Data - This line indicates whether your Guest and/or Master keys will encode additional data (such as the encoder and user) when the keys are made. This information can be read by Saflok for trouble shooting purposes. It can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

Password Sign On Time Out - This line indicates how frequently a user must re-enter their password when making keys or performing other transaction functions. It can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

SYSTEM HARDWARE SETTINGS - This section indicates the # of stations and station # of other hardware in your system. It can be changed using the 9.SYSTEM DESIGN - 1.SYSTEM HARDWARE function.

Max # of Stations - This is the # of encoders in your system contains.

System Printer - This is the terminal a printer is normally connected to for reports.

DATA FILE SIZING - This section indicates the maximum # of locks or keys your key design files are sized for and the actual # of locks and keys currently being used. It also indicates that you can have a maximum of 31 users in your system. You cannot change this information.

FAILSAFE KEYS - This section indicates the # of Failsafe sequences you should pre-make and store. It can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

GUEST KEYS - This section indicates information on guest key defaults and other related settings. The settings can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

NEW KEY WARNING - This section indicates the settings for prompting a warning that a new master key was recently made when you try to make another New key. The settings can be changed using the 9.SYSTEM DESIGN - 2.SYSTEM DEFAULTS function.

KEY EXPIRATION DEFAULTS - This section indicates the default settings that are used for key expiration for guest and master keys. Guest keys will add this time to the # of days entered for checkout and master keys will display the default days shown and allow you to change the # of days when you are making New Master keys.

Key Design Report 2 - Sample Report

Below is a sample of the Locks & Keys Assigned Report. Explanations of how to read it are provided on the following pages.

```
PAGE 1     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

LOCK & KEY DATA FILE DESIGN INFORMATION:  REPORT # 2
--------------------------------------------------------------------------------
Using PROPPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 1-42
Using NAMEINDX.ACT Vers: 06-14-2006  Prop#: 100   Seq: 7-0
Using KEYPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 2-7
Using LOCK_KEY.ACT Vers: 06-14-2006  Prop#: 100   Seq: 9-0

LOCKS & KEY ASSIGNMENTS:
Max # of Locks: 318    Current # of Locks: 145

HT = Hardware Types: 0=ECU/RCU, 1=ECU/RCU latching 2=Solenoid, 3=Motor
```

LOCK#	HT	ROOM	SUITE	LIMTD	FLSF	SECTN	FLOOR	LATCH	INHBT	GMSTR	EMERG	LCKOT	SPK	PPK
71	1	71	71	71	71	71	71	71	71	71	71	71	1	1
72	1	72	-	72	72	71	71	71	71	71	71	71	1	1
73	1	73	71	73	73	71	71	71	71	71	71	71	1	1
74	1	74	-	74	74	71	71	71	71	71	71	71	1	1
75	1	75	-	75	75	71	71	71	71	71	71	71	1	1
101	1	101	-	101	101	11	1	-	1	1	1	1	1	1
102	1	102	-	102	102	11	1	-	1	1	1	1	1	1
103	1	103	103	103	103	11	1	-	1	1	1	1	1	1
104	1	104	103	104	104	11	1	-	1	1	1	1	1	1
105	1	105	105	105	105	11	1	-	1	1	1	1	1	1
106	1	106	105	106	106	11	1	-	1	1	1	1	1	1
107	1	107	-	107	107	11	1	-	1	1	1	1	1	1
108	1	108	-	108	108	11	1	-	1	1	1	1	1	1
109	1	109	-	109	109	11	1	-	1	1	1	1	1	1
10P	1	Pass	Pass	Pass	Pass	11	1	-	1	1	1	1	1	1
111	1	111	-	111	111	12	1	-	1	1	1	1	1	1
112	1	112	112	112	112	12	1	-	1	1	1	1	1	1
114	1	114	112	114	114	12	1	-	1	1	1	1	1	1
115	1	115	115	115	115	12	1	-	1	1	1	1	1	1
116	1	116	115	116	116	12	1	-	1	1	1	1	1	1
117	1	117	-	117	117	12	1	-	1	1	1	1	1	1
118	1	118	-	118	118	12	1	-	1	1	1	1	1	1
119	1	119	-	119	119	12	1	-	1	1	1	1	1	1
120	1	120	-	120	120	12	1	-	1	1	1	1	1	1

Key Design Report 2 - Information Explanation

Report 2 allows you to print out all your locks with all the different keys that should work in each one.

At the top of the report, the maximum # of locks your key design files are sized for and the actual # of locks currently being used is indicated. In addition, an explanation of the HT column setting is provided.

The remainder of the report lists the locks that were in the range you requested. Each lock prints the following information:

LOCK# - This is the lock # or name used when programming locks and printed for Lock Interrogation reports.

HT - This is the lock hardware type used when programming the lock. If you replace a lock, you must use the same hardware type as indicated for the lock to function properly. The Hardware Types include:
0 - Multi channel ECU
1 - Motor lock with motor switch only and RCU units
2 - Solenoid lock (Select) which has no motor, but has a knob turn switch
3 - Motor lock which has a motor and a knob turn switch

ROOM through PPK keys - Each of these columns corresponds to the key or pass feature for each of the lock levels that should work in the lock.

If a key is mastered into a lock, its Key # is printed. These are also the numbers or names that would be entered when making the key and printed in Lock Interrogation reports.

If the pass feature is programmed into a lock level, "Pass" or "Pass1" through "Pass6" will be printed. "Pass" indicates that any key of the level will work in the lock. "Pass1" through “Pass 6” indicates the level was assigned a Pass number.

If there is no key for the level, a dash is printed.

Key Design Report 3 - Sample Report

Below is a sample of the Keys & Locks Assigned Report. Explanations of how to read it are provided on the following pages.

```
PAGE 1     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

LOCK & KEY DATA FILE DESIGN INFORMATION:  REPORT # 3
--------------------------------------------------------------------------------
Using NAMEINDX.ACT Vers: 06-14-2006  Prop#: 100   Seq: 7-0
Using KEYPROG.ACT Vers: 06-14-2006  Prop#: 100   Seq: 2-7
Using KEY-LOCK.ACT Vers: 06-14-2006  Prop#: 100   Seq: 1-0

KEYS & LOCK ASSIGNMENTS:

KEY LEVEL: SECTION        Max # of Keys: 30     Current # of Keys: 10
KEY # PASS#  LOCKS KEY IS ASSIGNED TO
----- -----  ------------------------------------------------------------
11      0    101   102   103   104   105   106   107   108   109   110
12      0    111   112   114   115   116   117   118   119   120
21      0    201   202   203   204   205   206   207   208   209   210
22      0    211   212   214   215   216   217   218   219   220
31      0    301   302   303   304   305   306   307   308   309   310
32      0    311   312   314   315   316   317   318   319   320
41      0    401   402   403   404   405   406   407   408   409   410
42      0    411   412   414   415   416   417   418   419   420
71      0    71    72    73    74    75
LC      0    LC1   LC2   LC3   LC4
```

Key Design Report 3 - Information Explanation

Report 3 allows you to print out all the different keys in your system with all the locks each key should work in.

At the top of the report, the key level is indicated and the maximum # of keys your key design files are sized for and the actual # of keys currently being used is indicated.

The remainder of the report lists the keys that were in the range you requested. Each key prints the following information:

KEY# - This is the room or key # or name used when making keys and printed for Lock Interrogation reports.

PASS# - This is the key's pass # which is used by locks with the pass feature programmed into the level. If a lock has "Pass" or "Pass1" through "Pass6" indicated for the key level in Report 2, it will look at the key's pass # to determine if the key should work. The Pass #s include:
0 - Pass All: The key will work in locks with "Pass"
1 – 6 - Pass # 1 through Pass # 6: the keys will work in locks assigned to that Pass number

LOCKS KEY IS ASSIGNED TO - This is a list of all the locks the key is assigned to and should work in. It does not list locks which use the pass feature for the key level. If there are no locks listed, the key will only work in locks with the pass function (see Pass # above).

10.5 USERS & AUTHORIZATIONS REPORT

10.5.1 Requesting the User & Authorization Report/View Function

This function will allow you to view a user's information, view all the users in your system or print all your users' information and the authorization group functions. If you want to change an person's user information or to view a user's password, refer to Section 9. This function can only be requested at the DeskLinc Main Terminal. If you select to print a report, it will require the System Printer to be connected and available. You will not be able to use the DeskLinc Main Terminal for any other functions until the report is finished.

There are two different reports that print in the Users & Authorization Report. Report 1 prints the users assigned in your system, including the user #, name, authorizations, date they were added and last date they were changed. It will not print passwords. Report 2 prints a listing of all the functions that each authorization group will allow a user to select.

Step 1. If you are at the Sign On screen, follow the steps in Section 10.1 to select the REPORTS MENU. The following screen will appear.

```
REPORT MENU:
1.TX HISTORY
2.KEY DESIGN
3.USERS & AUTH
```

Step 2. Press 3 or use the ARROW DOWN key to display the 3.USERS & AUTH menu item. Then press ENTER. If you are done viewing users and printing reports, press ESC to return to the Sign On screen.

```
REPORT MENU:
1.TX HISTORY
2.KEY DESIGN
3.USERS & AUTH
```

Step 3. If you want to view several users or User & Auth reports or other reports, we suggest you press 1. If you do, you will return to the REPORT MENU screen after you are done instead of returning all the way back to the Sign On screen.

```
Do you wish to Re-
peat this Function
when you are Done ?
Press 1=Yes or 0=No
```

Step 4. If you have authorization 1.ALL Auths or 8.User/Key Design, the following screen will appear.

```
USERS & AUTHS MENU:
1.View a User & Auth
2.View All Users
3.Print Users & Auth
```

If you want to view the user information of a particular user #, press 1 or use the ARROW keys to select 1.View a User & Auth. Then press ENTER. Then go to step 5.

If you want to view all the user #s and employees assigned to them, press 2 or use the ARROW keys to select 2.View All Users. Then press ENTER. Then go to step 9.

If you want to print the reports of all your users assigned and all the authorization group functions, press 3 or use the ARROW keys to select 3.Print Users & Auth. Then press ENTER. The computer will then try to print the report (go to step 10). This function will require the System Printer to be connected and available. You will not be able to use the DeskLinc Main Terminal for any other functions until the report is finished.

If you do not want to view any more users or print any more reports, press ESC to return to the Password/Sign On screen or the main Reports Menu:

- If you indicated 1=Yes in Step 3, you will now return to the REPORTS MENU screen (Step 1) and can select another report.

- If you indicated 0=No in Step 3, you will now return to the Password/Sign On screen.

Step 5. If you selected 1.View a User & Auth in step 4, the following screen will appear. You are now asked to enter the user # of the user you are interested in. Enter the user # (between 1 and 250) and press ENTER. If you are done viewing users, press ESC to return to Step 4.

```
011:VIEW USER & AUTH

User # (1-250): 0___
or ESC to Menu
```

Step 6. The following screen will now appear. This screen shows the employee who is assigned the to the User #. To display the next screen of information, press any key.

```
012:USER # 15
 John Doe

 ** PRESS ANY KEY **
```

Step 7. The following screen will now appear. This screen shows the date the user # was first assigned to an employee and the last date the employee name, password or authorizations were changed. To display the next screen of information, press any key.

```
013:USER # 15
Added:   03/21/95
Changed: 03/25/95
** PRESS ANY KEY **
```

Step 8. The following screen will now appear. This screen shows the authorization groups the user has. This is the last of the information displayed. When you press any key you will retune to Step 4.

```
013:USER # 15
Added:   03/21/95
Changed: 03/25/95
** PRESS ANY KEY **
```

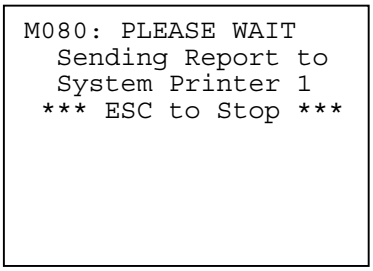
Step 9. If you selected 2.View All Users in step 4, the following screen will appear. This screen shows two users at a time and displays the employee who is assigned to each User #. The user #s are not displayed in numerical order. User 254 is the system user # which is used by the DeskLinc System to log automatic changes for station status and DST time changes.

To display the next 2 users, press any key.

To return to the Step 4 USER & AUTHS MENU, press ESC.

```
021:VIEW ALL USERS
254 System User
15  John Doe
** PRESS ANY KEY **
```

Step 10. If you selected 3.Print Users & Auth in step 4, the following screen should appear. Assuming your printer is connected to the Terminal and is not being used by another station, the terminal will display the following screen and will begin printing the report. You cannot use the terminal again until the report is done. If you have an emergency, you can press ESC to abort the report.



Step 11. When the report is done, or if you press ESC, you will return to the Step 4 USER & AUTHS MENU.

10.5.2 Reading the User & Authorization Report

Users & Authorizations Report 1 - Sample Report

Below is a sample of Report 1 of the Users & Authorizations Report. Explanations of how to read it are provided on the following page.

```
PAGE 1     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

USER & GROUP TX AUTHORIZATION REPORTS:  REPORT # 1  (MM-DD-YY)
-------------------------------------------------------------------------------
USERAUTH.ACT Vers: 11-15-2005
USER ASSIGNMENTS & AUTHORIZATIONS:
Currently 12 of 33 User #s Assigned

USER#  -----USER NAME-----  -AUTHORIZATIONS- ---1ST ADDED----  --LAST CHANGED--
 254   DESKLINC SYSTEM                      11-16-05 12:00AM  11-16-05 12:00AM
 250   SAFLOK REP           1               11-16-05 12:00AM  11-16-05 12:00AM
 1     ARTEEN-JASON           2 3           05-30-06 02:55PM  05-30-06 02:55PM
 2     JONES-MARSHA           2 3           05-30-06 02:55PM  05-30-06 02:55PM
 3     KELLOR-JACK            2 3           05-30-06 02:56PM  05-30-06 02:56PM
 4     MASTERSON-ANNE         2 3           05-30-06 02:57PM  06-03-06 10:13AM
 11    DICKENSON-ROD          2 3 4   6 7   05-30-06 02:57PM  05-30-06 02:57PM
 12    PETER-SUSAN            2 3 4   6 7   05-30-06 02:57PM  05-30-06 02:57PM
 13    CRAFT-ANITA            2 3 4   6 7   05-30-06 02:57PM  05-30-06 02:57PM
 51    GARRET-MARY          1               05-30-06 02:57PM  05-30-06 02:57PM
 52    EDWARDS-GENE         1               05-30-06 02:57PM  05-30-06 02:57PM
 100   PMS INTERFACE          2 3           06-17-06 08:59AM  06-17-06 08:59AM
```

Users & Authorizations Report 1 - Information Explanation

The Users & Authorizations Report 1 prints all the users in the system including their user #, employee name, authorizations, date added and last date changed.

At the top of the report, the # of users currently assigned and the maximum # of users allowed is printed.

The remainder of the report prints all the user information. Each user # will print the following:

USER # - This is the # printed in the Tx History Report to identify which user performed a function. It is also the # you must enter in the 7.AUTHORIZE USERS function to change, view or delete the user.

USER NAME - This is the name of the employee assigned to the user #.

AUTHORIZATIONS - This identifies the authorization groups the user has. The Authorization Group report lists the functions that each group allows a user to perform.

1ST ADDED - This indicates the date & time that an employee was first assigned to a user #. To ensure that it always corresponds to the date & time an employee was first allowed to perform transaction functions, you must make sure you do not simply change the name of an employee assigned to a user # when adding a new user. You should first delete an old employees user # information and then add the user # back for the new employee (see Section 9).

LAST CHANGED - This indicates the last date & time that the user #s employee name, password or authorizations were changed.

Authorization Groups Report 2 - Sample Report

Below is a sample of Report 2 of the Users & Authorization Report. Explanations of how to read it are provided below.

```
PAGE 2     06-30-2006  11:22AM DST    DESKLINC SYSTEM           TERMINAL # 1

USER & GROUP TX AUTHORIZATION REPORTS:  REPORT # 2  (MM-DD-YY)
--------------------------------------------------------------------------------
GRPAUTH.ACT Vers: 11-15-2005
GROUP AUTHORIZATIONS:

GRP# 1: ALL AUTHORIZATIONS
  All functions listed in all groups

GRP# 2: FRONT DESK
  New & Dupl Room & Suite Keys

GRP# 3: ADDITIONAL FRONT DESK
  Override Error Capability for New & Dupl Room & Suite Keys
  Checkout Room & Suite Keys
  Limited Use Key
  Tx History Report
  Key Design Report

GRP# 4: FAILSAFE KEYS
  New & Dupl Failsafe Keys

GRP# 5: MASTER KEYS
  New & Dupl Master Keys
  PPK & SPK Keys
  Status & Display Keys
  Tx History Report
  Key Design Report

GRP# 6: INTERROGATE LOCKS
  Interrogate Locks
  Program Lock Clock Date & Time

GRP# 7: PROGRAM LOCK
  Program Locks

GRP# 8: USER/KEY DESIGN
  Change System Hardware
  Change System Defaults
  Authorize Users
  Set System Date & Time
  Set System DST Settings
  Tx History Report
  Key Design Report
  User & Auth Display & Report

GROUPS 1,2,4,5 & 8 ALSO INCLUDES THE FOLLOWING:
  Set Terminal Settings
  Tests & Clear Printer
  Communications Changes
  Display Station Info
  Exit Program
```

User & Group Authorization Report 2 - Information Explanation

The User & Group Authorization Report 2 prints all 8 possible authorizations groups that can be assigned and lists the transaction functions that each group allows a user to perform.

SECTION 11 - SETTING THE SYSTEM DATE, TIME & DST

11.1 ENTERING THE SYSTEM DATE & DST MENU

In order to do any of the functions listed in this section, you will need to first sign on and select the Additional Menu and System Date & DST function from the Terminal's Sign On screen.

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

Step 3. Press 6 or use the ARROW DOWN key to display 6.ADDITIONAL MENU. Then press ENTER.

```
Room #________
Checkout in 1  days
Make 1  keys –max 99
3.NEW SUITE KEY
4.DUPL SUITE KEY
5.LIMITED USE KEY
6.ADDITIONAL MENU
    More Options
```

Step 4. The following ADDITIONAL MENU screen will appear. Press 8 or use the ARROW DOWN key to display the 8.SYSTEM DATE & DST menu item. Then press ENTER.

```
ADDITIONAL  MENU:
2.DUPL MASTER KEYS
3.CHECK OUT A KEY
4.MISCELLANEOUS KEYS
6.REPORTS
7.AUTHORIZE USERS
8.SYSTEM DATE & DST
    More Options
```

Step 5. If you are authorized, the following menu will appear. From this menu you can select any of the functions listed in this section.

```
SYSTEM DATE & DST:
1.SYSTEM DATE & TIME
2.DST SETTINGS
```

11.2 SETTING THE SYSTEM DATE & TIME

This function will allow you to view and/or change the system date & time. It is important that the date & time be accurate because it will be used to program the locks' clocks and to determine proper key expiration.

Step 1. If you are at the Sign On screen, follow the steps in Section 11.1 to select the SYSTEM DATE & DST menu. The following screen will appear.

```
SYSTEM DATE & DST:
1.SYSTEM DATE & TIME
2.DST SETTINGS
```

Step 2. Press 1 or use the ARROW UP key to display the 1. SYSTEM DATE & TIME menu item. Then press ENTER.

```
SYSTEM DATE & DST:
1.SYSTEM DATE & TIME
2.DST SETTINGS
```

Step 3. If you are authorized for 8.User/Key Design, the following screen will appear. The current date, time and DST (daylight savings time) or STD (standard time) status will be displayed.

```
SYSTEM DATE & TIME
03/31/95 10:17AM STD
Change Date & Time ?
Press 1=Yes or 0=No
```

If the system date & time is correct, press 0 or ESC to abort and exit the function. You will then return to the Password or Sign On. If you need to correct the date or time, press 1 for Yes and continue to Step 4. If you have not set your Daylight Savings Time (DST) information yet, the DST or STD information next to the time will not be correct. To correct it, you must follow the steps in Section 11.3. This should be done before you set the date & time if possible. If you were forced to set the date & time, you may have to set the date & time first and then again after you set the DST info.

Step 4. If you pressed 1 to change the date & time, the following screen will appear. The original date information will be displayed as defaults for each entry. If you like the value, you can simply press ENTER. Otherwise, enter the new value and then press ENTER.

```
001:ENTER NEW DATE:
Month (1-12) 3__
Date  (1-31) 3_1_
Year         1_9_9_5
```

Remember that you can hold down the SHIFT key and press the ARROW UP key to backspace if you make a mistake and you can use the ARROW UP key to move back up to a previous input field.

Step 5. After you press ENTER for the year, if the date is valid, the following screen will appear. The original time information will be displayed as defaults for each entry. If you like the value, you can simply press ENTER. Otherwise, enter the new value and then press ENTER.

```
001:ENTER NEW DATE:
Hour  (1-12) 1_0_
Mins  (0-59) 1_7_
AM (0) or PM (1) 0_
```

Remember that you can hold down the SHIFT key and press the ARROW UP key to backspace if you make a mistake and you can use the ARROW UP key to move back up to a previous input field.

Step 6. After you press ENTER for the AM/PM option, the following screen will appear. The new date, time and DST (daylight savings time) or STD (standard time) status will be displayed.

```
003: NEW DATE & TIME
MM-DD-YY HH:MM A/PM
IS THIS CORRECT?
Press 1=Yes or 0=No
```

If the new system date & time is correct, press 1 for Yes and continue to Step 7.

If the new system date & time is incorrect, press 0 for No. You will then return to step 4.
If you have not set your Daylight Savings Time (DST) information yet, the DST or STD information next to the time will not be correct. To correct it, you must follow the steps in Section 11.3. This should be done before you set the date & time if possible. If you were forced to set the date & time, you may have to set the date & time first and then again after you set the DST info.

Step 7. If you pressed 1 indicating the date & time were correct, the following screen will appear.

```
M220: Do You want to
Save the Changes ?

Press 1=Yes or 0=No
```

If you want to save the new system date & time, press 1 for Yes and continue to Step 8. If you want to abort the function without saving the new system date & time, press 0 for No. You will then return to Step 4.

Step 8. If you pressed 1 to save the new date & time, one of the following screens will appear if the new date and time was much different the original date and time. If neither screen appears, the date & time will be set and you will return to the Password or Sign On screen.

Message 221: If the new date you entered is early than the original date, you will get Message 221. This message indicates that for any locks that you made new keys for in the last xxx days, you will want to reprogram the locks as soon as you can and replace the keys you made. This is because the keys will now have a future date on them and will expire at a later date in the future. If you make new keys again before reprogramming the locks affected, you will keep getting an error message indicating that the last new key made date is greater than the current date and time. This will continue for the # of days indicated in Message 221 or until you reprogram the lock.

```
M221: New Keys made
in last xxxxx days
need ReProgram Locks
** PRESS ANY KEY **
```

When you press any key, the date & time will be changed and you will return to the Password or Sign On screen.

Message 222 If the new date you entered is more than 7 days later than the original date, you will get Message 222. This message is warning you that you may have entered something incorrectly and requires you to verify that the new date you entered is correct.

```
M222: mm/dd/yy IS
OVER 7 DAYS BEYOND
ORIGINAL. Okay ?
Press 1=Yes or 0=No
```

If it is correct, press 1 and the date & time will be changed. If it is incorrect, press 0 for No and the date & time will be NOT be changed. You will then return to the Password or Sign On screen.
If you have locks installed, you should also update their clocks (see Section 8.3).

11.3 SETTING THE SYSTEM DAYLIGHT SAVINGS TIME INFORMATION

You should reset the DST information when you first receive your DeskLinc System or if you ever receive a key design change or replacement Terminal. If your area uses a non-standard method (see Option 3) for determining when DST changes occur, you will also be forced to reset the DST information on Jan 1 of every year. You will then have to update every lock's clock to program in the new DST information. The locks will automatically indicate their clocks need updating on January 1.

This function will allow you to view and/or change the dates that Daylight Savings Time is in effect. It is important that the DST information be accurate because it will be used to program the locks' DST change information. The DST information will be programmed into the lock when it is programmed, interrogated or its clocks is updated. The DeskLinc computer and the locks will automatically add or subtract and hour from their date and time based on the DST information.

You must first determine the appropriate DST Option that applies to your location. The DST Options and how they work are listed below. You can then perform the transaction function.

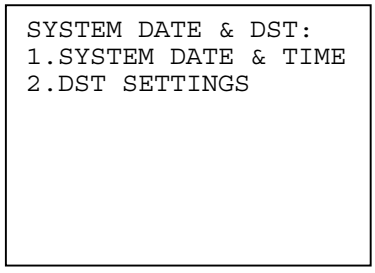
DST OPTION 0 - This option indicates that Daylight Savings time never goes into effect for your location. The time always stays on normal standard time year round.

DST OPTION 1 - This option is for Standard U.S. Time Changes.
Every year, DST Starts on the first Sunday in April at 2:00AM.
Every year, DST Ends on the last Sunday in October at 2:00AM.
Note: for the Southern Hemisphere, start & end dates are reverse of this.

DST OPTION 2 - This option is for Standard Local Time Changes. If your area does not use the Standard U.S. changes (Option 1) or the Standard U.S. date or time changes listed in Option 1 are changed by the government, this option would need to be used.
Every year, DST Starts on a certain month, day of week, week of month and time.
Every year, DST Ends on a certain month, day of week, week of month and time.

DST OPTION 3 - This option is for Non-Standard Local Time Changes. If your area's DST changes do not fall under option 1 or 2, you must select Option 3 and enter the actual dates and times that DST changes occur every year.
Every year, DST Starts on a different month, day of week, week of month and time.
Every year, DST Ends on a different month, day of week, week of month and time.
Note: This option will require you to enter new DST change dates every January 1 and then reprogram all locks' clocks with the new DST information.

Step 1. If you are at the Sign On screen, follow the steps in Section 11.1 to select the SYSTEM DATE & DST menu. The following screen will appear.



Step 2. Press 2 or use the ARROW key to display the 2. DST SETTINGS menu item. Then press ENTER.

```
SYSTEM DATE & DST:
1.SYSTEM DATE & TIME
2.DST SETTINGS
```

Step 3. If you are authorized for 8.User/Key Design, one the following screens will appear. The current DST Option will be displayed and if DST applies, the dates it starts and ends will be displayed. The example on the left is for DST Option 1.

SCREEN IF DST APPLIES

```
CURRENT DST OPTION 1
STR 04/02/2006 2:00A
END 10/29/2006 2:00A
Change DST Info ?
```

SCREEN IF DST DOESN'T APPLY

```
CURRENT DST OPTION 4
DST Doesn't Apply

Change DST Info?
```

If the DST information is correct, press 0 or ESC to abort and exit the function. You will then return to the Password or Sign On. If you need to correct the DST Option or the dates or times it changes, press 1 for Yes and continue to Step 4.

Step 4. If you pressed 1 to change the DST information, the following DST CHANGE MENU screen will appear.

```
DST CHANGE MENU
1.Change DST Option
2.Change DST Dates
```

If you are setting up all your DST information, press 1 and ENTER. Then go to step 5.

If you doing this function because you have Option 3 and are forced to update the information on January, you simply need to update the DST dates. Press 2 and ENTER, then go to step 9.

Step 5. If you pressed 1 to change the DST Option, the following DST OPTION MENU screen will appear.

```
DST OPTION MENU
1.Stnd U.S. Changes
2.Stnd Local Changes
3.Non-Standard Chngs
4.DST Doesn't Apply
```

You must now select the appropriate DST Option for your location. Refer to the beginning of this section for details of each option.
For DST Option 1, press 1 and ENTER. Then go to step 6.
For DST Option 2, press 2 and ENTER. Then go to step 6.
For DST Option 3, press 3 and ENTER. Then go to step 6.
For DST Option 4, press 4 and ENTER. Then go to step 11.

Step 6. If you selection DST option 1, 2 or 3, the following screen will appear.

```
Does DST Start and
End in the Same Year
(North Hemisphere) ?
Press 1=Yes or 0=No
```

If you are located in the Northern Hemisphere, press 1.
If you are located in the Southern Hemisphere, press 0.

If you selected DST option 1, go to step 11.
If you selected DST option 2, go to step 7.
If you selected DST option 3, go to step 9.

Step 7. If you selected DST Option 2, one of the following screens will now appear for the first DST time change. If you indicated you are located in the Northern Hemisphere, the screen on the left will appear. If you indicated you were located in the Southern Hemisphere, the screen on the right will appear.

NORTHERN HEMISPHERE

```
STRT Month (1-12) __
Day of Wk (1-7)   _
Wk of Month (1-6) _
Hour (0-23)       __
```

SOUTHERN HEMISPHERE

```
END  Month (1-12) __
Day of Wk (1-7)   _
Wk of Month (1-6) _
Hour (0-23)       __
```

For the Northern Hemisphere, you will be entering information on when DST STARTS.
For the Southern Hemisphere, you will be entering information on when DST ENDS.
- First enter the month (1-12) and press ENTER.
- Next enter the day of week (1=Sun, 2=Mon, 3=Tue, 4=Wed, 5=Thu, 6=Fri, 7=Sat) and press ENTER.
- Next enter the week of the month or occurrence (1-6) and press ENTER. For example, assuming the change occurs on Sunday, is it the 1st Sun of the month, the 2nd or the last (=6).
- Now enter the hour of the day that DST changes (0-23) and press ENTER. The hour must be military time: 0 is midnight, 12 is noon and 13 through 23 are 1 PM through 11 PM.

After pressing ENTER for the hour, go to step 8.

Step 8. If you selected DST Option 2, one of the following screens will now appear for the second DST time change. If you indicated you are located in the Northern Hemisphere, the screen on the left will appear. If you indicated you were located in the Southern Hemisphere, the screen on the right will appear.

NORTHERN HEMISPHERE

```
END  Month (1-12) __
Day of Wk (1-7)   _
Wk of Month (1-6) _
Hour (0-23)       __
```

SOUTHERN HEMISPHERE

```
STRT Month (1-12) __
Day of Wk (1-7)   _
Wk of Month (1-6) _
Hour (0-23)       __
```

For the Northern Hemisphere, you will be entering information on when DST ENDS.
For the Southern Hemisphere, you will be entering information on when DST STARTS.
- First enter the month (1-12) and press ENTER.
- Next enter the day of week (1=Sun, 2=Mon, 3=Tue, 4=Wed, 5=Thu, 6=Fri, 7=Sat) and press ENTER.
- Next enter the week of the month or occurrence (1-6) and press ENTER. For example, assuming the change occurs on Sunday, is it the 1st Sun of the month, the 2nd or the last (=6).
- Now enter the hour of the day that DST changes (0-23) and press ENTER. The hour must be military time: 0 is midnight, 12 is noon and 13 through 23 are 1 PM through 11 PM.

After pressing ENTER for the hour, go to step 11.

Step 9. If you selected DST Option 3, one of the following screens will now appear for the first DST time change. If you indicated you are located in the Northern Hemisphere, the screen on the left will appear. If you indicated you were located in the Southern Hemisphere, the screen on the right will appear.

NORTHERN HEMISPHERE

```
030:ENTER STRT INFO:
Month (1-12) __
   Date (1-31)  __
Hour (0-23)  __
```

SOUTHERN HEMISPHERE

```
030:ENTER END INFO:
Month (1-12) __
Date (1-31)  __
Hour (0-23)  __
```

For the Northern Hemisphere, you will be entering information on when DST STARTS.
For the Southern Hemisphere, you will be entering information on when DST ENDS.
- First enter the month (1-12) and press ENTER.
- Next enter the date of the month (1-31) and press ENTER.
- Now enter the hour of the day that DST changes (0-23) and press ENTER. The hour must be military time: 0 is midnight, 12 is noon and 13 through 23 are 1 PM through 11 PM.

After pressing ENTER for the hour, go to step 10.

Step 10. If you selected DST Option 2, one of the following screens will now appear for the second DST time change. If you indicated you are located in the Northern Hemisphere, the screen on the left will appear. If you indicated you were located in the Southern Hemisphere, the screen on the right will appear.

NORTHERN HEMISPHERE

```
030:ENTER END INFO:
Month (1-12) __
Date (1-31)  __
Hour (0-23)  __
```

SOUTHERN HEMISPHERE

```
030:ENTER STRT INFO:
Month (1-12) __
Date (1-31)  __
Hour (0-23)  __
```

For the Northern Hemisphere, you will be entering information on when DST ENDS.
For the Southern Hemisphere, you will be entering information on when DST STARTS.
- First enter the month (1-12) and press ENTER.
- Next enter the date of the month (1-31) and press ENTER.
- Now enter the hour of the day that DST changes (0-23) and press ENTER. The hour must be military time: 0 is midnight, 12 is noon and 13 through 23 are 1 PM through 11 PM.

After pressing ENTER for the hour, go to step 11.

Step 11. If you set the DST information, one of the following screen will appear. The new DST Option will be displayed and if DST applies, the dates it starts and ends will be displayed. The example below is for DST Option 1.

SCREEN IF DST APPLIES

```
CURRENT DST OPTION 1
STR 04/02/1995 2:00A
END 10/29/1995 2:00A
Change DST Info ?
```

SCREEN IF DST DOESN'T APPLY

```
CURRENT DST OPTION 4
DST Doesn't Apply

Change DST Info?
```

If the new DST information is correct, press 1 for Yes and continue to Step 12.
If the new DST information is NOT correct, press 0 or ESC. If you press 0, you will return to step 3 and can try resetting the information again. If you press ESC, you will abort and exit the function. You will then return to the Password or Sign On.

Step 12. If you press 1 in step 11 to indicate the new the DST information is correct, the following screen will appear. If you have any locks that are already programmed, this reminds you that you must now update all the locks' clocks so they have the new DST information (see Section 8.3). When you press any key, you will end the function and return to the Password or Sign On screen.

```
M250: You should now
  Program ALL Locks'
  Clock Date & Time
 ** PRESS ANY KEY **
```

SECTION 12 - MISCELLANEOUS TERMINAL FUNCTIONS

12.1 ENTERING THE MISCELLANEOUS MENU

In order to do any of the functions listed in this section, you will need to first sign on and select the Miscellaneous function from the Terminal's sign on screen.

Step 1. At the Sign On screen, enter your 3-10 character password (if needed) and press ENTER.

Step 2. Press ENTER three times to move the cursor to the transaction menu.

Step 3. Press 9 or use the ARROW DOWN key to display the 9. MISCELLANEOUS menu item. Then press ENTER.

```
Password ****____
Room # __________
Checkout in 2 days
Make 1  keys -max=99
6.ADDITIONAL MENU
7.PROGRAN LOCKS
8.INTERROGATE LOCKS
9.MISCELLANEOUS
    More Options
```

```
Room # __________
Checkout in 2 days
Make 1  keys -max=99
6.ADDITIONAL MENU
7.PROGRAN LOCKS
8.INTERROGATE LOCKS
9.MISCELLANEOUS
0.IDENTIFY A KEY
    More Options
```

Step 4. The following MISCELLANEOUS MENU screen will appear. From this menu, you can select any of the functions listed in Section 12.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINT
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Miscellaneous Menu Selections
1. TESTS/CLEAR PRINTR
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM

12.2 CLEAR TERMINAL PRINTER ERRORS

This function is seldom used except for troubleshooting. It will allow you to clear any Terminal printer errors or reservations. It can also be used to run special troubleshooting tests. These tests are not covered here since they would only be done with instruction from a SAFLOK Service Representative.

If a Terminal is having trouble communicating with its station printer, you may be instructed by service personnel to do this function. It only affects the Terminal you run this function at. If the Terminal "thinks" it has a station printer and that printer is reserved for a printout, it will not allow you to select the printer unless the terminal that reserved it unreserves it. Or you can run this function to clear the printer reservation.

Step 1. Follow the steps in Section 12.1 to select the MISCELLANEOUS MENU. The following MISCELLANEOUS MENU screen will appear.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINTR
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

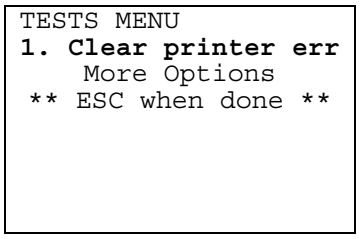
Step 2. Press 1 or use the ARROW UP key to display the 1. TESTS/CLEAR PRINTR menu item. Then press ENTER.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINTR
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

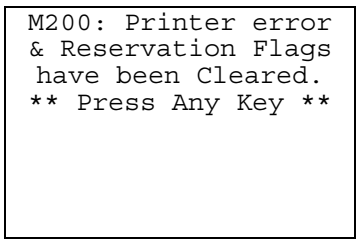
Step 3. The following TESTS MENU screen will appear.

```
TESTS MENU
1. Clear printer err
    More Options
 ** ESC when done **
```

Step 4. At the TESTS MENU screen, press 1 or use the ARROW UP key to select 1. Clear Printer Err, then press ENTER. Or press ESC to return to the Sign on screen.



Step 5. The terminal will clear all its printer reservation and error flags and will display the following message. Press any key to return to the TESTS MENU screen.



12.3 COMMUNICATIONS (RESTART, CLEAR BUSY STATION, ETC.)

This function is seldom used except for troubleshooting. It will allow you to clear an encoder that is busied out (K198: ENCODER BUSY) or to restart the terminal's communications with its encoder. To select the menu, which allows you to do these functions, follow these steps:

12.3.1 Selecting the COMMUNICATIONS Menu Function.

Step 1. Follow the steps in Section 12.1 to select the MISCELLANEOUS menu item. The following MISCELLANEOUS MENU screen will appear.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINT
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 2. Press 2 or use the ARROW DOWN key to display the 2. COMMUNICATIONS menu item. Then press ENTER.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINT
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 3. The following menu will appear. You can now select one of the functions or press ESC to return to the sign on screen. DeskLinc Main Terminals and Front Desk Terminals have different menu selections. Refer to Sections 12.3.1 to 12.3.5 for the additional function steps.

```
COMMUNICATIONS MENU
1. Restart Sta Commun
2. Clear Station Busy
3. Master Reassign
4. Disable Sta Commun
 ** ESC when done **
```

DeskLinc Termianl
Menu Selections
1. Restart sta commun
2. Clear station busy
3. Master reassign
4. Disable station commun

Front Desk Terminal
Menu Selections
1. Restart station commun
2. Clear station busy

12.3.2 Restarting Station Communications

If a Terminal is having trouble communicating with its encoder, you may be instructed by service personnel to do this function. This function causes the Terminal to shut down and restart communications. If this is done at the DeskLinc Terminal, it will then cause all other stations to re-sign onto it. If it is done at a Front Desk Terminal, only that terminal will re-sign on to the Main.

Steps 1-3. Follow the steps in Section 12.3.1 Selecting the COMMUNICATIONS menu function.

Step 4. At the COMMUNICATIONS MENU screen, press 1 or use the ARROW UP key to select 1. Restart Sta Commun, then press ENTER. Or press ESC to return to the Sign on screen.

```
COMMUNICATIONS MENU
1. Restart Sta Commun
2. Clear Station Busy
3. Master Reassign
4. Disable Sta Commun
 ** ESC when done **
```

Step 5. If the terminal is a DeskLinc Main Computer, the following message will then be displayed. It is mainly to warn you that it will cancel any functions currently being done at other stations and then cause them to re-sign on.

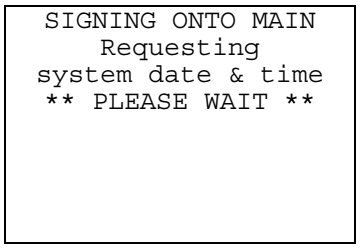
```
M220: THIS WILL MAKE
ALL STATIONS RE-SIGN
    ON. Continue?
 Press 1=Yes or 0=No
```

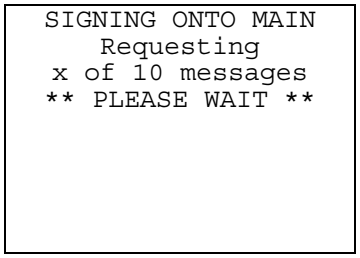
If you press 0, you will simply return to the COMMUNICATION MENU again. If you press 1, the terminal will send a message to the encoder to restart communications and will display the following message.

Step 6. For both terminal types, the following screen will then appear and the terminal will send a message to the encoder to restart communications. If the message stays on the screen for more than a few seconds, it indicates that the terminal is having trouble communicating with the encoder.

```
  M221: PLEASE WAIT
 Restarting Station
   Communications
 ** ESC to abort **
```

Step 7. The Front Desk Terminal will then display the following messages as it tries to sign back on to the DeskLinc Main computer. There are a total of 11 message screens. If any of these messages display for more than a few seconds each, it typically indicates the terminal can communicate with its encoder, but the encoder cannot communicate with the DeskLinc Main computer. If a message stays on for 15 to 20 seconds, the terminal will display an error message to suggest what is wrong.

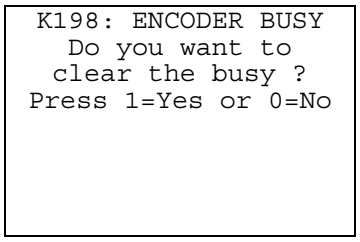




Step 8. If the communications restart is successful, the Terminal will display the COMMUNICATIONS MENU again. You can select any function in the menu or press ESC to return to the Sign On screen.

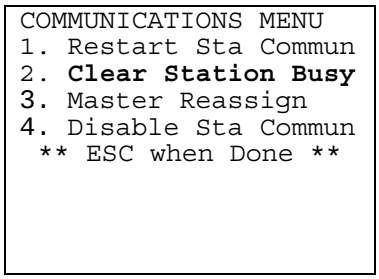
12.3.3 Clearing the K198: ENCODER BUSY Error

The error screen shown below would occur when you try to make keycards. This occurs when the encoder is reserved by the Terminal or through the PMS Interface to make keys. After making the keys, the encoder should be unreserved by the Terminal or PMS Interface. If for some reason this did not occur, the error will continue to occur. If the error message is on the screen, you can simply press 1 to try to clear the error. If it does not clear, you can reset the encoder's power. If the terminal is at a Sign On screen, you can follow this procedure to clear the problem.

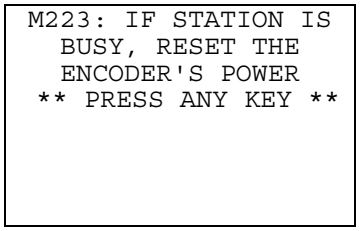


Steps 1-3. Follow the steps in 12.3.1 Selecting the COMMUNICATIONS Function.

Step 4. At the COMMUNICATIONS MENU screen, use the ARROW DOWN key or press 2.Clear Station Busy, then press ENTER.



The terminal will send a message to the encoder to unbusy itself and then display the following message:



Step 5. Reset power to the encoder (disconnect then reconnect the power cord at the back of the encoder). The terminal will automatically re-start communications with the encoder and cause any other stations to re-sign back on after the encoder comes on line again.

Press ESC until you return to the sign on screen. You should now be able to make keys without getting the STATION BUSY error message.

12.3.4 Reassigning the Terminal as the Main Computer

This function is only used for troubleshooting. The DeskLinc Main Computer Terminal automatically starts up assigned as the Main in the system. If for any reason, a communications problem occurs to cause it to be unassigned, this function will reassign it as the Main again.

Steps 1-3. Follow the steps in 12.3.1 Selecting the COMMUNICATIONS Function.

Step 4. At the COMMUNICATIONS MENU screen, press 3 or use the ARROW DOWN key to select 3.Master Reassign, then press ENTER. Or press ESC to return to the Sign on screen if you are done.

```
COMMUNICATIONS MENU
1. Restart Sta Commun
2. Clear Sta Busy
3. Master Reassign
4. Disable Sta Commun
  **ESC when Done**
```

Step 5. If the following message is displayed, it indicates the DeskLinc Terminal was already assigned as the Main. When you press any key, you will simply return to the COMMUNICATION MENU again.

```
 E202: THIS STATION
  IS ALREADY A MAIN

** PRESS ANY KEY **
```

Step 6. If the following message is displayed, it indicates the DeskLinc Terminal was unassigned and has now been reassigned as the Main. The DeskLinc Terminal will have sent a message to the encoder to be the Main. Any other stations on the network will also re-sign on to the DeskLinc Main. When you press any key, you will simply return to the COMMUNICATIONS MENU again.

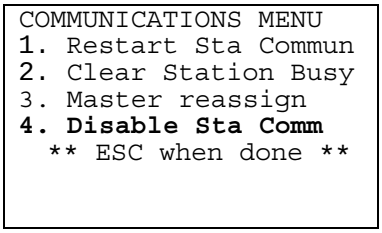
```
E224: STATION 1  IS
  REASSIGNED AS MAIN

 ** PRESS ANY KEY **
```

12.3.5 Disabling Station Communications

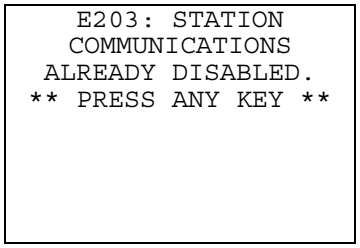
This function is only used for troubleshooting. It will disable station communications between the DeskLinc Terminal and its encoder. If this is done, no functions can be performed on any station in the system until communications is restarted.

Steps 1-3. Follow the steps in 12.3.1 Selecting the COMMUNICATIONS Function.

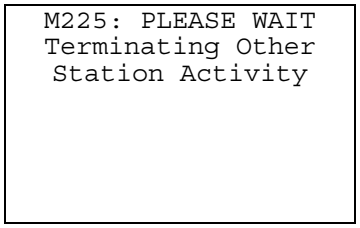
Step 4. At the COMMUNICATIONS MENU screen, press 4 or use the ARROW DOWN key to select 4.Disable Sta Comm, then press ENTER. Or press ESC to return to the Sign on screen if you are done.

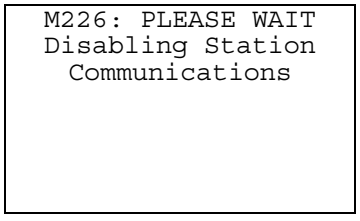


Step 5. If the following message is displayed, it indicates the station communications was already disabled. When you press any key, you will simply return to the COMMUNICATIONS MENU again.



Step 6. If the station communications was not already disabled, the following screens will be displayed and you will simply return to the COMMUNICATIONS MENU again. This may happen so quickly that you do not even see the screens. The DeskLinc Terminal will have sent a message to the encoder to disable communications.





12.4 TERMINAL SETTINGS

This function is seldom used except for initial system setup and troubleshooting. It will allow you to assign the terminal printer, make the network selection and select the LPI probe type. To select the menu, which allows you to do these functions, follow these steps:

12.4.1 Selecting the TERMINAL SETTINGS Menu Function

Step 1. Follow the steps in Section 12.1 to select the MISCELLANEOUS MENU. The following MISCELLANEOUS MENU screen will appear.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINT
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 2. Press 3 or use the ARROW DOWN key to display the 3. TERMINAL SETTINGS menu item. Then press ENTER.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINT
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 3. The following menu will appear. You can now select one of the functions or press ESC to return to the sign on screen. Refer to sections 12.4.2, 12.4.3 or 12.4.4 for the additional function steps.

```
TERMINAL SETTINGS
1. Terminal Printer
2. Network Selection
3. LPI Probe Type

 *** ESC to exit ***
```

12.4.2 Setting the Terminal Printer Option

This function lets you indicate if a printer can be connected to the terminal.

Steps 1-3. Follow the steps in 12.4.1 Selecting the TERMINAL SETTINGS Menu Function.

Step 4. At the TERMINAL SETTINGS menu screen, press 1 or use the ARROW UP key to select 1.Terminal Printer, then press ENTER. Or press ESC to return to the Sign on screen.

```
TERMINAL SETTINGS
1. Terminal Printer
2. Network Selection
3. LPI Probe Type

 *** ESC to exit ***
```

Step 5. The following menu will be displayed. The cursor will flash on the current setting.

```
PRINTER CONNECTED
1. To Terminal
2. No Printer
```

If you need or want to change the setting, use the following guidelines to make the proper selection. Then enter the selection # and press ENTER. If you do not want to change the setting, just press ESC. You will then return to the TERMINAL SETTINGS menu. You can then select another function or press ESC to return to the Sign On screen.

1. To Terminal: Printer can be connected to the printer port at the top of the Terminal.

2. No Printer: No printer will be connecter to the terminal.

Step 6. If you selected option 1. To Terminal the following screen will appear. Press 0 for Open Drain then press ENTER.

```
Set Printer Output
      Type? 0
(0 = Open Drain)
(1 = Totem Pole)
 Press Enter or ESC
```

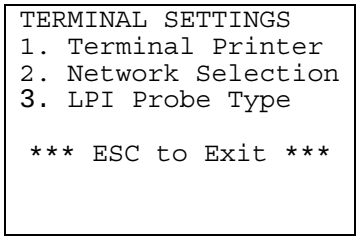
You will then return to the TERMINAL SETTINGS menu. You can then select another function or press ESC to return to the Sign On screen.

12.4.3 Network Selection

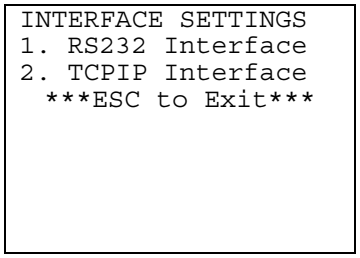
This function allows you to select the type of network you will be using.

Steps 1-3. Follow the steps in 12.4.1 Selecting the TERMINAL SETTINGS Menu Function.

Step 4. At the TERMINAL SETTINGS menu screen, press 2 or use the ARROW UP key to select 2. Network Selection, then press ENTER. Or press ESC to return to the Sign on screen.



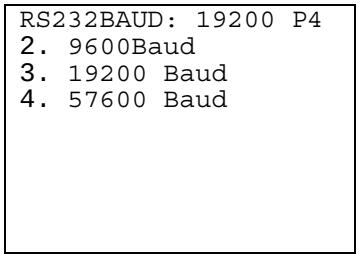
Step 5. The following menu will be displayed. The cursor will flash on the current setting.



If you would like to change the setting use the ARROW UP or AROW DOWN to position the cursor on the setting you want, then press ENTER.

For details on option 1. RS232 Interface, go to step 6.
For details on option 2. TCP/IP Interface refer to Section1.4 Settin Up A Multi Station System.

Step 6. If you selected 1. RS232 Interface the following screen will appear. At the top of the screen, the current baud rate set in the unit will display.



If you need or want to change the setting, use the following guidelines to make the proper selection. Then enter the selection # and press ENTER. If you do not want to change the setting, just press ESC. You will then return to the TERMINAL SETTINGS menu. You can then select another function or press ESC to return to the Sign On screen.

Baud Rate Options:

1. 4800 Baud: This setting will not be used with the DeskLinc System.

2. 9600 Baud: This setting will be used if the terminal will communicate with the Property Management System.

3. 19200 Baud: This setting will be used if the terminal will be connected to an insertion encoder.

4. **57600 Baud:** This setting will be used if the terminal will be connected to a motorized encoder.

12.4.4 Setting the LPI Probe Type

This function allows you to set the type of probe that your locks will use.

Steps 1-3. Follow the steps in 12.4.1 Selecting the TERMINAL SETTINGS Menu Function.

Step 4. At the TERMINAL SETTINGS menu screen, press 3 or use the ARROW DOWN key to select 3. LPI Probe Type, then press ENTER. Or press ESC to return to the Sign on screen.

```
TERMINAL SETTINGS
1. Terminal Printer
2. Network Selection
3. LPI Probe Type

 *** ESC to Exit ***
```

Step 5. The following menu will be displayed.

```
SELECT LPI PROBE
1. SMARTCARD
2. BLACK MAG
Override system = 1
```

If your property will *only use* the Smartcard probe, place the cursor on 1 and then press ENTER. The cursor will move the Override system prompt. Type 0, then press ENTER.

If your property will *only use* the Black Mag probe, put the cursor on 2 and then press ENTER. The cursor will move the Override system prompt. Type 0, then press ENTER.

If your property will *use both* the Smartcard and Black Mag probes, place the cursor on 1 and then press ENTER. The cursor will move the Override system. Enter 1, then press ENTER. When programming or interrogating the terminal will give you the option to select the probe type you are currently using.

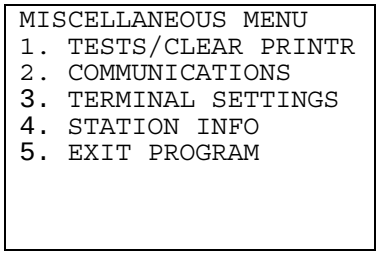
The screen will return to the TERMINAL SETTINGS menu. Press ESC to exit to the Password or Sign On screen.

12.5 STATION INFO (SOFTWARE VERSIONS, STATION #, DATE & TIME)

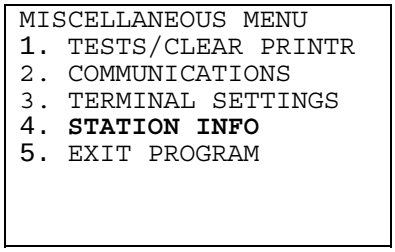
This function is used to verify your Terminal software, Max Stations in your network, System Printer station, Terminal station # and encoder software versions. To select the menu which allows you to do these functions, follow these steps:

12.5.1 Selecting the STATION INFO Menu Function.

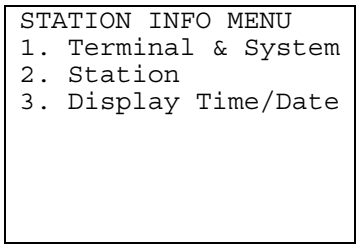
Step 1. Follow the steps in Section 12.1 to select the MISCELLANEOUS MENU. The following MISCELLANEOUS MENU screen will appear.



Step 2. Press 4 or use the ARROW DOWN key to display the 4. STATION INFO menu item. Then press ENTER.



Step 3. The following menu will appear. You can now select one of the functions or press ESC to return to the sign on screen. Refer to sections 12.5.2, 12.5.3 or 12.5.4 for the additional function steps.



12.5.2 Display Terminal & System Info

This function lets you display the Terminal's Software Version, the Max Stations in your System and the System Printer Station #. The software version will allow you to tell if a Terminal is a DeskLinc Computer Terminal or a Front Desk Terminal and whether it has been updated with the latest software version or not. If you add a station and do not "tell" the DeskLinc Main computer to increase the Max Stations, the station will not be able to communicate with the new station. The System Printer station # tells you which Terminal to connect the System Printer to (see also 12.4.2 for how to connect a System Printer).

Steps 1-3. Follow the steps in 12.5.1 Selecting the STATION INFO menu function.

Step 4. At the STATION INFO MENU screen, press 1 or use the ARROW UP key to select 1.Terminal and System, then press ENTER. Or press ESC to return to the Sign on screen.

```
STATION INFO MENU
1. Terminal & System
2. Station
3. Display Time/Date
```

Step 5. The following information screen will be displayed.

DeskLinc Terminal

```
HHVersion DCA5:mmddyy
Max Stations n
System Printer # x
  ** PRESS ANY KEY **
```

Front Desk Terminal

```
HHVersion DFA5:mmddyy
Max Stations n
System Printer # x
  ** PRESS ANY KEY **
```

When you are done viewing the information, press any key. You will then return to the STATION INFO MENU. You can then select another function or press ESC to return to the Sign On screen.

1st Line: Displays the Terminal 's software version.
DCA5 indicates it is a DeskLinc Computer Terminal.
DFA5 indicates it is a Front Desk Terminal.
"mmddyy" is the software version date.

2nd Line: Displays the Max Stations "n" in the system. This can only be changed at the DeskLinc Computer terminal.

3rd Line: Displays the System Printer station # "x". The System Printer should typically connected to the DeskLinc Terminal station # 1. This can only be changed at the DeskLinc Computer terminal.

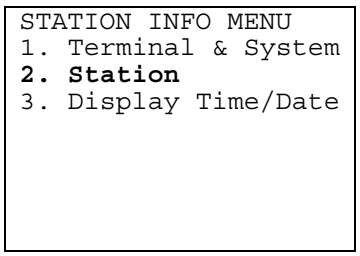
The max stations and system printer station can be changed using the DeskLinc Computer terminal. Refer to Section 15.1 for instructions.

12.5.3 Display Station Info

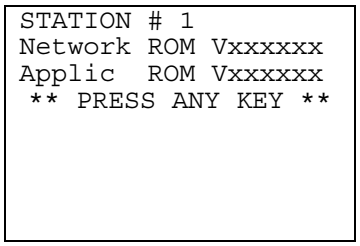
This function lets you display information related to the encoder connected to the Terminal. It includes the Terminal's and Encoder's station # and the Encoder ROM software versions. The software version will allow you to tell if an Encoder has been updated or not.
The Terminal station # indicates the encoder's station setting so you can verify it to avoid duplicating station #s and verify if the station matches the System Printer (see also 12.4.2 for how to connect a System Printer).

Steps 1-3. Follow the steps in 12.5.1 Selecting the STATION INFO Menu Function.

Step 4. At the STATION INFO MENU screen, press 2 or use the ARROW DOWN key to select 2.Station, then press ENTER. Or press ESC to return to the Sign on screen.



Step 5. The following information screen will be displayed.



When you are done viewing the information, press any key. You will then return to the STATION INFO MENU. You can then select another function or press ESC to return to the Sign On screen.

1st Line: Displays the Terminal's and Encoder's station #.
The DeskLinc Computer Terminal should always be station # 1.
The Front Desk Terminals should always be between 2 and 10.
(No two encoders should have the same station #.)

2nd Line: Displays the Encoder's Network ROM software version.
"xxxxxx" is the software version.

3rd Line: Displays the Encoder's Application ROM software version.
"xxxxxxx" is the software version.

12.5.4 Display Terminal Date & Time

This function lets you display the Terminal's date and time. The Terminal gets this information from the Main computer whenever it signs on or whenever the System Date and Time or Daylight Savings Time (DST) is updated at the DeskLinc Main computer. If the date or time is incorrect, it must be updated at the Main computer.

Steps 1-3. Follow the steps in 12.5.1 Selecting the STATION INFO MENU Function.

Step 4. At the STATION INFO MENU screen, press 3 or use the ARROW DOWN key to select 3. Display Time/Date, then press ENTER. Or press ESC to return to the Sign on screen.

```
STATION INFO MENU
1. Terminal & System
2. Station
3. Display Time/Date
```

Step 5. The following date and time screen will be displayed. If Daylight Savings Time is in effect, the time will be followed by "DST". The date is always displayed in the MM/DD/YY format (month/date/year) and the day of week is also displayed.

```
System Time & Date
    10:10A DST
    04/15/94 Sat
** Press Any Key **
```

When you are done viewing the information, press any key. You will then return to the STATION INFO MENU. You can then select another function or press ESC to return to the Sign On screen.

If the date or time is incorrect, you should exit to the Password / Sign On screen and follow the Steps in Section 11.2 to reset the system date and time. Note: You must do this at the DeskLinc Main Computer Terminal.

If the time and DST status is incorrect, you should exit to the Password / Sign On screen and follow the Steps in Section 11.3 to check and/or reset the system DST information. Note: You must do this at the DeskLinc Main Computer Terminal.

12.6 EXIT PROGRAM

This function is used to exit the program to the POWER UP MENU. If you are going to load or unload files or disconnect the Hand-Held unit in order to move, store or ship it, you should first exit the program. When you exit the program, the terminal will return to the POWER UP MENU (see Section 13.4). If you exit the program at your main DeskLinc Computer Terminal, you will not be able to use any Front Desk Terminals again until you restart the DeskLinc Computer's program.

Step 1. Follow the steps in Section 12.1 to select the MISCELLANEOUS MENU. The following MISCELLANEOUS MENU screen will appear.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINTR
2. COMMUNICATIONS
2. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 2. Press 5 or use the ARROW DOWN key to display the 5. EXIT PROGRAM menu item. Then press ENTER.

```
MISCELLANEOUS MENU
1. TESTS/CLEAR PRINTR
2. COMMUNICATIONS
3. TERMINAL SETTINGS
4. STATION INFO
5. EXIT PROGRAM
```

Step 3. The first screen will appear as the files are saved. When the second screen appears, press any key to exit the program. If you do not want to exit the program, simply press ESC to return to the sign on screen.

```
     Please Wait
Transferring files to
ROM.  This may take
a few Minutes.
```

```
S001: EXIT PROGRAM
TO POWERUP MENU.
Press Any Key or
Press ESC to Abort.
```

Step 4. If you press any key, different things will happen depending on whether the terminal is a DeskLinc Main Terminal or a Front Desk Terminal.

DESKLINC MAIN COMPUTER TERMINAL: The DeskLinc Main Computer Terminal will display the following screens when it ends all current functions that are running and then disables communications with its encoder. These functions may happen so quickly that you will not notice the first two screens being displayed.

```
M200: PLEASE WAIT
Terminating other
station activity
```

```
M202: PLEASE WAIT
Disabling station
communications
```

```
DCA5 POWER UP MENU
1. Start Program
2. Terminal Settings
3. Display Version
4. Load/Upload Files
5. Restart ROM COde

    More Options
```

FRONT DESK TERMINAL: The Front Desk Terminal will display the following screens when it logs off the Main computer and then disables communications with its encoder. These functions may happen so quickly that you will not notice the first two screens being displayed.

```
  M201: PLEASE WAIT
    Logging end of
      transaction
```

```
  M202: PLEASE WAIT
  Disabling station
    communications
```

```
DFA5 POWER UP MENU
1. Start program
2. Terminal settings
3. Display version
```

You are now ready to run a function from the POWER UP MENU or to disconnect the Hand-Held unit from the encoder.

APPENDIX A - SERVICE & SUPPORT INFORMATION

A.1 TECHNICAL SUPPORT AND CONTACTS

Listed below is the address and phone numbers to our office. Office hours are 8:30am to 5:00pm Eastern Time. Technical Support is available 24/7/365.

SAFLOK.
1950 Austin
Troy, MI 48083
Tel: (800) 999-6213 (service)
or (248) 680-8484 (main #)
Fax: (248) 680-8468

A.2 RETURN MATERIALS (RMA) PROCEDURES

If you need to return materials for servicing, you must contact the appropriate RMA personnel and obtain a Return Material Authorization (RMA) #. To ensure you will have spare locks or parts when needed, you should obtain an RMA # and return the material needing servicing as soon as possible. The Lock and Computer RMA departments are available during normal office hours at (800) 999-6213.

All packages sent to the RMA departments must be marked on the outside of the package with the RMA # in large bold print. Please be sure to properly pack and insure your packages. C.S.S. will not be responsible for equipment damaged in shipping or lost shipments.

A.3 ADDITIONAL ORDERING PROCEDURES

If you wish to order additional equipment or supplies, you should call 800.999.6213 during normal business hours and follow the menu prompts for parts and supplies.

TABLE OF CONTENTS

SUBJECT **PAGE NO.**

TABLE OF CONTENTS

SUBJECT **PAGE NO.**

SECTION 4 - GUEST KEYS

SECTION 5 - MASTER KEYS

SECTION 6 - FAILSAFE KEYS

TABLE OF CONTENTS

SUBJECT **PAGE NO.**

SECTION 7 - MISC SPECIAL KEYS FOR TROUBLESHOOTING

SECTION 8 - PROGRAMMING & INTERROGATING LOCKS

SECTION 9 - UPDATING USERS AND AUTHORIZATIONS

TABLE OF CONTENTS

SUBJECT **PAGE NO.**

SECTION 9 - UPDATING USERS AND AUTHORIZATIONS (continued)

SECTION 10 - REPORTS

SECTION 11 - SETTING THE SYSTEM DATE, TIME AND DST

SECTION 12 - MISCELLANEOUS TERMINAL FUNCTIONS

TABLE OF CONTENTS

SUBJECT **PAGE NO.**

DeskLinc System

OPERATIONS MANUAL